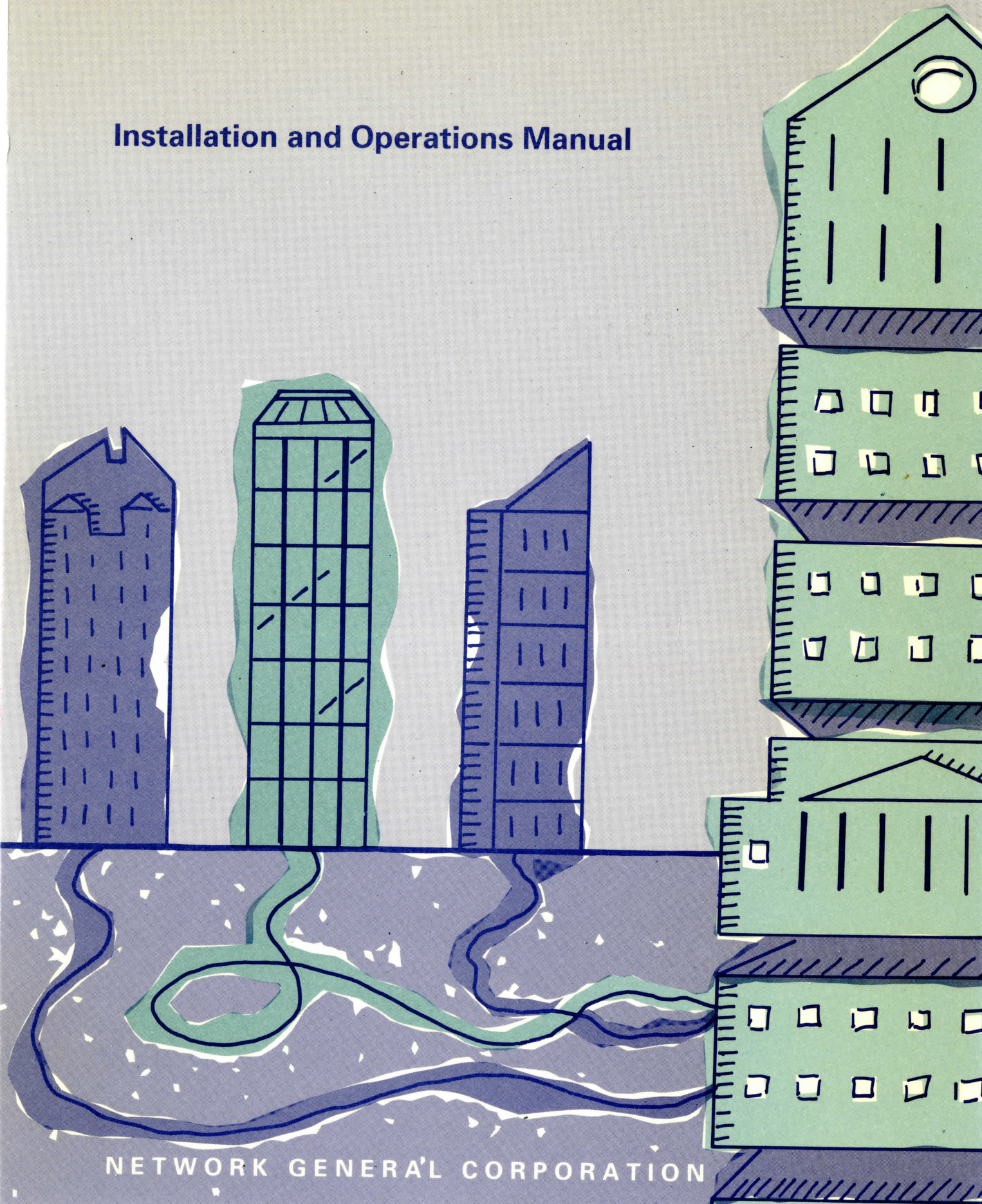
DISTRIBUTED SNIFFER SYSTEM™

Installation and Operations Manual



NETWORK GENERAL CORPORATION

DISTRIBUTED SNIFFER SYSTEM™

Installation and Operations Manual

NETWORK GENERAL CORPORATION

DISCLAIMER OF WARRANTIES

The information in this document has been reviewed and is believed to be reliable; nevertheless, Network General Corporation makes no warranties, either expressed or implied, with respect to this manual or with respect to the software and hardware described in this manual, its quality, performance, merchantability, or fitness for any particular purpose. The entire risk as to its quality and performance is with the buyer. The software herein is transferred "AS IS."

Network General Corporation reserves the right to make changes to any products described herein to improve their function or design.

In no event will Network General Corporation be liable for direct, indirect, incidental or consequential damages at law or in equity resulting from any defect in the software, even if Network General Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Document prepared by David M. Trousdale with contributions from Terri Fitzmaurice, Florence Chan, and Paul Berry.
May 1991

P/N: 20048-001

Table of Contents

List of Figures

Preface

Chapter 1. Distributed Sniffer System Overview

Chapter 2. Before You Begin

Chapter 3. Installation and Configuration

Chapter 4. Operation of the Distributed Sniffer System

Chapter 5. SNMP Network Management Stations in the System

Appendix A. Troubleshooting Guide

Appendix B. Troubleshooting and Fine Tuning Utilities

List of Procedures

PREFACE

Preface

About This Manual

This manual describes the installation and operations of the Distributed Sniffer System™. It also gives recommendations on configuring system components and on fine-tuning the system for thorough monitoring and analysis of your network.

The Distributed Sniffer System consists of two types of product: Sniffer® servers and SniffMaster™ consoles. Each server observes the local or wide-area network to which it's attached; consoles control servers and display the results of the servers' activities. Some servers run the monitoring and analysis applications alone, while others run both. Other manuals describe the monitoring and analysis applications.

Manuals for the Distributed Sniffer System

Two types of manual accompany the Distributed Sniffer System. The primary manuals, which include this one, describe the system's normal operations; the supplementary manuals describe the programs that configure and test the system's various hardware and software components for troubleshooting. The actual manuals in your shipment depend on the system configuration.

Figure i describes the primary manuals for the Distributed Sniffer System.

For Information On...	Read...
Installing and configuring servers and consoles. Operating consoles.	*Distributed Sniffer System: Installation and Operations Manual* or *Sniffer Server Installation Manual.*
Operating the server's analysis functions on an Ethernet, token ring, or wide area network.	*Distributed Sniffer System: Analyzer Operations Manual.*
Operating the server's monitor functions on a token ring network. Using the monitor features effectively to detect network abnormalities.	*Distributed Sniffer System: Token Ring Monitor Operations Manual.*
Operating the server's monitor functions on an Ethernet network. Using the monitor features effectively	*Distributed Sniffer System: Ethernet Monitor Operations Manual.*
Various network and protocol types.	*Distributed Sniffer System: Network and Protocol Reference.*

Figure i. Primary manuals for the Distributed Sniffer System.

Figure ii describes the supplementary manuals for the Distributed Sniffer System.

For Information On...	Read...
Running the adapter diagnostics to test the IBM 16/4 token ring adapter in the console.	*Token-Ring Network Guide to Operations.*
Running the diagnostics to test the InterLan NI5210 Ethernet controller in the console.	*NI5210 Installation Manual.*
Configuring and using the IBM® Local Area Network (LAN) Support Program.	*Local Area Network Support Program, User's Guide.*

Figure ii. Secondary manuals for the Distributed Sniffer System.

If the product shipment includes release notes or README files on disks, the information in the notes or files supersedes the information in this manual.

Audience of This Manual

The manual has been prepared with the following assumptions:

- You are a network manager or troubleshooter who understands how networks operate.
- You are familiar with DOS.

Organization of This Manual

Figure iii describes the organization of this manual.

Chapter/Appendix	Contents
Chapter 1, "Distributed Sniffer System Overview"	Provides an overview of the Distributed Sniffer System and describes its capabilities.
Chapter 2, "Before You Begin"	Describes information to know and actions to take before installing, configuring and operating the system.
Chapter 3, "Installation and Configuration"	Describes the installation and configuration of consoles and servers and how to establish connections.
Chapter 4, "Operations of the Distributed Sniffer System"	Describes how to control servers using SniffMaster consoles and how to configure the various mechanisms for presenting system information.
Chapter 5, "SNMP Network Management Stations"	Describes integration of the Distributed Sniffer System with your SNMP Network Management Stations.
Appendix A, "Troubleshooting Guide"	Provides recommendations for systematically isolating and correcting problems with your Distributed Sniffer System.
Appendix B, "Troubleshooting and Fine Tuning Utilities"	Describes each of the tools and utilities provided to help you troubleshoot and fine tune your Distributed Sniffer System.
Appendix C, "Configuration Record"	Discusses recommendations for keeping a detailed and accurate record of your Distributed Sniffer System.

Figure iii. The organization of the manual, Distributed Sniffer System: Installation and Operations Manual.

Navigational Aids Used in This Manual

To help you find procedures easily, a separate list of procedures is provided in this manual in addition to the Table of Contents and List of Figures. Also, the "Recommendation" entries in the Index point you to suggestions for getting the most from your Distributed Sniffer System.

This manual uses icons in the margin to help you locate important information as explained below:

The paragraph next to this icon contains information that is especially important. Read it carefully before you proceed.

A warning gives you instructions that you must follow to avoid possible damage to data files, program files, or hardware devices.

A cautionary paragraph provides information that you need to avoid injury to yourself or others.

A recommendation describes a useful and valuable way of using the products.

A procedure is a series of steps for accomplishing a particular task.

Conventions Used in This Manual

Special Notations

The following describes the conventions used in this manual:

Bold	Menu options are in bold type. For example: Move to **Display**, and press Enter.
UPPERCASE	Filenames and commands you type at a DOS prompt are in uppercase. For example: Modify the AUTOEXEC.BAT file if necessary. To duplicate the file, use the COPY command.
Bold italics	Variables, for which you insert values, are in bold italics. For example: Type the number of minutes and seconds in the *mm:ss* format.
`Screen font`	Screen messages are printed in monospaced font. For example: If a monitoring session is in progress, the following message appears: `You must stop monitoring before you can use this feature.`

ITEM1\ITEM2	A menu title made up from the succession of menu items chosen to get to the submenu. For example, to choose the **Interval** for a rotating carousel display, you would go to the Screen Carousel\Rotating Display menu.

Terminology

Hexadecimal numbers in the manual are followed by "(hex)"; numbers without any notations are decimal. For example, "The maximum number of stations is 75. The default memory address is D8000 (hex)."

The terms "monitor" and "analyzer" refer to software applications that run on token ring or Ethernet Sniffer servers. The term "console" refers to control and display software running on a dedicated PC.

Screen Displays and Keyboard Input

Enter all the keystrokes mentioned in the manual from the SniffMaster console. Similarly, all the screen displays generated by a server appear on the console's screen.

The screen displays in this manual may not be identical with what you see on your console screen. For example, you can choose to have the console show the server name on each monitor display, but the screens in this manual do not show the name.

Other Sources of Information

Network General Corporation (NGC) provides other sources of information that can help you get familiar with the Distributed Sniffer System.

On-Line Help

After highlighting an item in a console, analyzer, or monitor menu, you can see a phrase or sentence in a panel near the bottom of the screen. It explains the meaning of the highlighted item.

To obtain general information about a particular feature of the Distributed Sniffer System, press F1 at any time. A window containing a list of topics opens. If you are displaying a monitor statistics screen, pressing F1 gives you information on the current screen.

For detailed instructions, see "Using On-Line Help" on page 4–10.

Tutorial

NGC distributes a booklet with an accompanying diskette entitled *Real Networks, Real Problems.* It presents case studies using data captured with a Sniffer network analyzer from four different networks. The Sniffer analyzer and the server's analysis application have different capabilities, but the case studies allow you to see how investigation of a network problem proceeds.

You can obtain the tutorial free of charge from any of the company's sales representatives or directly from NGC.

Technical Support

A toll-free number is available to obtain technical support for the Distributed Sniffer System. Before calling, however, please check Appendix A., "Troubleshooting Guide." You will find tips for troubleshooting your system before requesting help as well as information you will need to provide when you do request help.

CHAPTER ONE: DISTRIBUTED SNIFFER SYSTEM 1

Chapter 1. Distributed Sniffer System Overview

Chapter Overview

This chapter summarizes the features of Network General's Distributed Sniffer System components, describes how the system works, shows several possible system configurations, and lists the major benefits of the system.

What the Distributed Sniffer System Is

A Distributed Sniffer System consists of *SniffMaster consoles* controlling network monitoring and analysis tools known as *Sniffer servers*.You can see a simple Distributed Sniffer System illustrated in Figure 1–1.

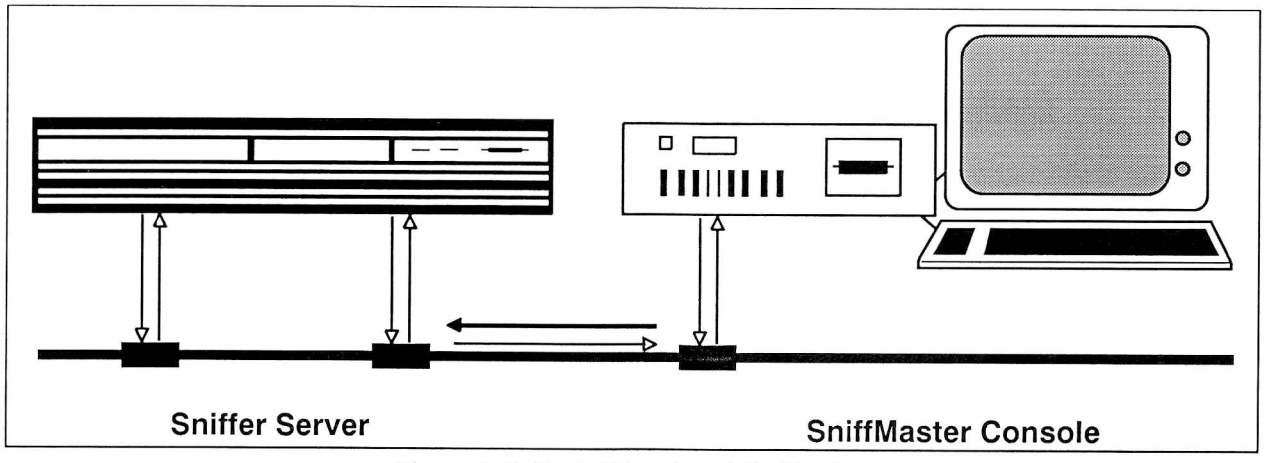


Figure 1–1. Basic Distributed Sniffer System components.

Servers are small and powerful computers with special applications software and hardware components that allow them to communicate with consoles, to collect statistics from the network, and to capture frames. They provide the processing power to give you a sophisticated view of your network, its problems and trends. You can have up to two consoles viewing and controlling one server.

Consoles connect to your servers and allow you to observe your network and control the servers' activities. They are also computers with a special software application and a board for communicating with servers. A console's display not only lets you inspect the individual Ethernet® segments, token rings, and wide area network (WAN) links to which servers are connected but also provides global information on your entire network.

You can set up the Distributed Sniffer System components on different segments, rings, and links of your network. Theoretically, you can have any number of SniffMaster consoles attached to different segments or rings, but no more than two consoles can simultaneously control any one server. The number of Sniffer servers you can control from one console will vary according to the configuration of your particular Distributed Sniffer System.

What the Distributed Sniffer System Can Do

The Distributed Sniffer System allows you to optimize performance and to troubleshoot problems within and between distributed local area networks (LANs) from a SniffMaster console. Information from multiple network segments, rings, or links observed by Sniffer servers is relayed to the SniffMaster console. From the console, you can see what is happening anywhere on your network through a rotating display on the SniffMaster console's screen. Furthermore, you can alter options on any of the Sniffer servers whenever you want. The distributed network system gives you a powerful set of tools for monitoring and analyzing your network.

Sniffer servers on each network segment, ring, or link are the eyes and the intelligence of the system. Each Sniffer server operates as a station on the LAN and allows you to look into the LAN, to observe trends, to recognize simple and complex problems, and to locate their sources quickly. SniffMaster consoles display network information that servers see and interpret, and consoles let you control the servers so they can provide complete network information.

The Sniffer family of diagnostic tools helps maintain, troubleshoot, fine-tune, and expand a network. The two primary applications of Sniffer servers are seven-layer protocol decoding and traffic monitoring that includes statistical displays, alarms, and report generation.

How the Distributed Sniffer System Works

This section briefly describes how the Distributed Sniffer System works. Refer to the appropriate chapters and manuals for detailed information on installing, configuring, and operating each of the products used in the system.

The Sniffer Server

Figure 1–1 shows the basic components of the Distributed Sniffer System. On the left-hand side of the diagram, you see a Sniffer server. It contains network monitoring and analysis applications software

(Figure 1–4). In addition, it has a powerful microprocessor, a hard disk, and two network interface cards (NICs): the *Monitor Card* and the *Transport Card.*

The Monitor Card is used for analyzing or monitoring network traffic—e.g., collecting data from which statistics are calculated, setting off alarms, and capturing frames for analysis. When connected to the SniffMaster console, a server regularly transmits what it knows about its network to the SniffMaster console via the Transport Card.

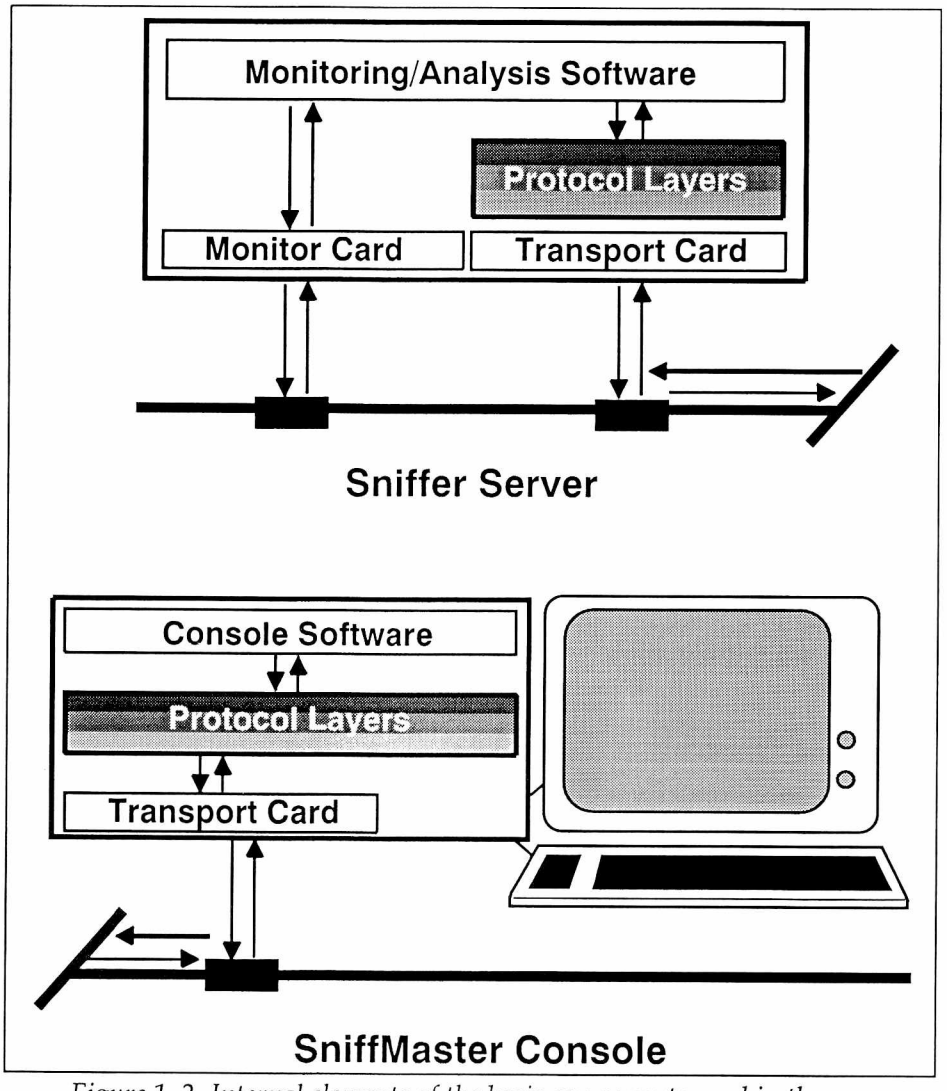


Figure 1–2. Internal elements of the basic components used in the Distributed Sniffer System.

Sniffer server software applications are of two types:

- Monitoring application
- Analysis application.

A *monitoring application*—that is, the network monitoring program installed either in a Sniffer monitor server or in a Sniffer analysis server—continuously maintains a set of real-time counters, charts and summaries of network activity. A monitor continuously scans a list of possible warning thresholds and transmits alarms to the console when they're encountered.

An *analysis application*—that is, the network analyzing program installed in a Sniffer analysis server—records and interprets network transmissions. The work of analysis occurs in two stages:

Capture: The analyzer records network traffic for later interpretation. Capture can be filtered to record only traffic meeting certain criteria. Capture can be frozen when a triggering condition is observed to assure that the retained sample includes traffic just before or after the event of interest.

Display: The analyzer interprets the recorded traffic. During display, the analyzer decodes the various layers of protocol in the recorded frames and displays them as English abbreviations or summaries. The analyzer can filter the display to show only those frames that meet certain criteria.

The SniffMaster Console

The SniffMaster console uses its own Transport Card to receive network information from the Sniffer servers (Figure 1–4). It displays that information on its own display as screens of individual servers, or it consolidates information—for example, alarms signalling problems and other significant conditions on different network segments and rings—from all connected servers.

The user also controls the servers from the console. The console transmits keystrokes entered on its keyboard to servers to start and stop functions, to reformat displays, or to change applications.

Protocol Layers in Servers and Consoles

Consoles and servers talk to each other using a transport protocol. Figure 1–3 shows the possible protocol and network interface combinations used in servers and consoles.

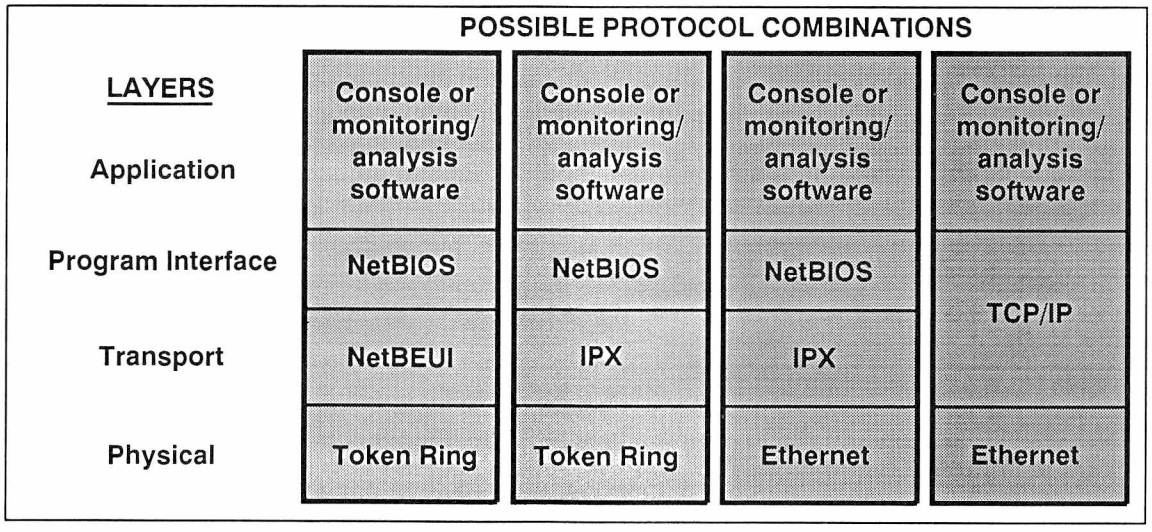


Figure 1–3. Protocol layers used in the Distributed Sniffer System.

The transport layer you choose is very important. Transport protocols make communication between consoles and servers possible in a distributed environment. In the Distributed Sniffer System, the three transport protocols available are NetBEUI, Novell's IPX, and TCP/IP. It is necessary that all servers and consoles in one Distributed Sniffer System use the same transport protocol.

Internetworking Devices and the Distributed Sniffer Environment

The different network segments, rings and links may be connected to one another with various types of *internetworking devices*. Some internetworking devices–*repeaters*, for instance–are unimportant as far as the protocols that are used.

The use of other internetworking devices has significant consequences. *Bridges* may do "protocol filtering" that stops packets of certain types from passing through them. *Routers* need to be able to "talk" a specific protocol before they will let that protocol's packets pass through. *Gateways* convey data from one protocol stack to another. Therefore, the type of internetworking devices being used in your network determines the appropriate transport protocol.

Distributed Sniffer System Configurations

Figure 1–4 shows you several possible configurations within a Distributed Sniffer System. Your Sniffer servers can keep an eye on Ethernet, token ring, or WAN traffic. Each Sniffer server sends what it sees in the traffic it observes to the SniffMaster console through a TCP/IP, IPX, or NetBEUI connection over Ethernet or token ring.

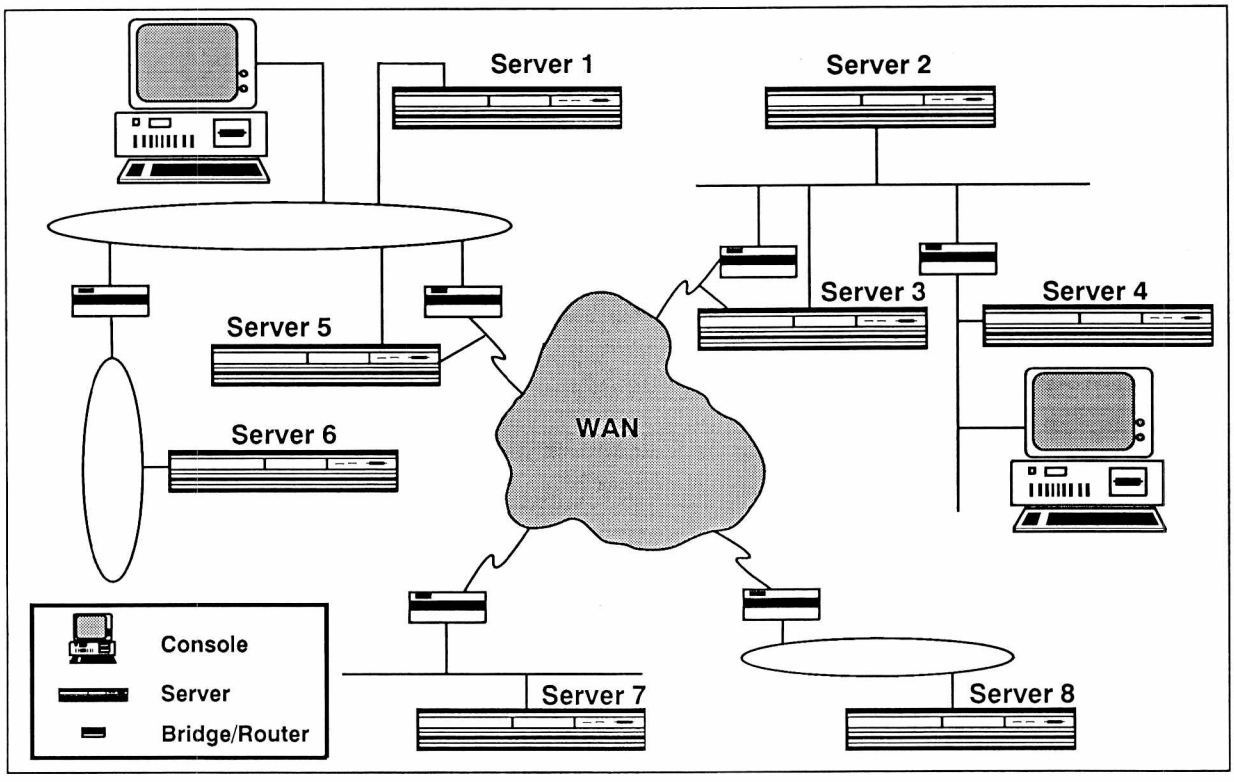


Figure 1–4. Example of a Distributed Sniffer System.

Figure 1–4 shows a number of the possible ways of linking Sniffer servers and SniffMaster consoles to make a Distributed Sniffer System. Servers 1 and 5 are connected to the same token ring as one of the consoles. Server 1 observes that ring whereas Server 5 observes the WAN link. Server 6 observes yet another ring and can communicate with the console through a bridge or router. Servers 2 and 3 are connected to the same Ethernet segment. Server 2 observes that segment while Server 3 observes a WAN link. Both can communicate with the first console via the WAN or with the second console via a bridge or router. Server 8 observes a token ring and can be controlled by either console via the WAN.

Benefits of the Distributed Sniffer System

The Distributed Sniffer System has several useful benefits. One is consolidated management of distributed LANs and WAN links. You can analyze and monitor many local and remote LANs from a SniffMaster console. This lets you utilize scarce networking expertise more effectively and provides for quicker problem resolution with quick access to any segment, ring, or WAN link.

Another capability is simultaneous monitoring and analysis of multiple LANs and WAN links. Using the rotating screen display on

the SniffMaster console, you can view statistics and analyze network traffic on several segments, rings, and links at a time.

Security is available for the Sniffer servers. Each Sniffer server controlled by a SniffMaster console can be password-protected to prevent unauthorized use. Also Sniffer servers are without keyboards and displays to prevent tampering with, or access to, network information.

With the system, you can analyze network data on the SniffMaster console. You can transfer user-selected network data directly to the SniffMaster console for printing, display, or analysis by additional network management tools.

CHAPTER TWO: BEFORE YOU BEGIN 2

Chapter 2. Before You Begin

Chapter Overview

This chapter provides unpacking instructions, first time precautions, the system requirements, a list of documentation, and advice on protecting your system.

Unpacking

Unpack each Distributed Sniffer System component from its carton. The items in the cartons may include:

- One or more SniffMaster consoles, turnkey or board-and-software versions
- Multiple Sniffer servers
- Cabling
- Documentation
- License agreement
- Warranty registration cards
- Configuration sheets. These describe the specific configuration for a server or a console.
- Packing lists. These describe all items included in the shipment, and there's an identical one in each box.

Verify the items you received against the packing lists.

Read the license agreement. If you cannot accept its terms, go no further! You have three days to put everything back into the boxes and to return the items. When you connect a server or turnkey console to a power outlet or install a board-and-software version of the console, you are signaling that you accept the terms of the license agreement.

Fill out the warranty registration cards, and return them to Network General Corporation.

First Time Precautions

As soon as possible, make backups of important SniffMaster console and Sniffer server files before monitoring, capturing, or analyzing data. You can easily protect yourself from a disaster by preparing a

few diskettes in advance. Follow these procedures to ensure the safety of your software and data:

- If you purchased a turnkey SniffMaster console, you will want to back up everything on the hard disk to diskettes (see "To back up the entire hard disk of the SniffMaster console:" on page 2–13).
- If you don't want to do a full hard disk backup, you can limit the backup to a particular directory (see "To limit a backup to a particular directory:" on page 2–15).
- If you've completed the installation and configuration of a Sniffer server, you will want to back up certain files on the server's hard disk (see "To back up critical files on an installed, configured, and connected Sniffer server:" on page 2–15).

Also note that each server comes with a label attached to the bottom with important information about the unit, e.g., serial number, hardware address, and so on. There are also extra labels with the same information on them. When you put a server on a rack or in a closet, you will want to put an extra label in a highly visible place so that you can identify the unit and refer to the information whenever you want. Also you will want to record the information in some other place. See "System Configuration Record" on page C–3.

System Requirements

This section describes the hardware and software components that you must have before you can run the Distributed Sniffer System.

SniffMaster Console

The SniffMaster console comes in two configurations: a *board-and-software* version and a *turnkey* version. Both of these basic configurations come in various combinations of Transport Card and transport protocol.

Board-and-Software Version

The SniffMaster console board-and-software version requires the following hardware and software components to be supplied by the user:

- 80386- or 80486-based PC with:

  Minimum of 4MBytes of RAM

  60MByte hard disk

  Either a 1.2MByte (5.25") or a 1.44MByte (3.5") floppy drive

One available Industry Standard Architecture (ISA) or Extended Industry Standard Architecture (EISA) bus interface card slot (for the Transport Card)

- Enhanced PC keyboard with 12 function keys
- VGA color monitor and interface
- MS/PC-DOS 3.3 or later.

Turnkey Version

The SniffMaster turnkey console version comes equipped with:

- Compaq DeskPro 386/25e
- 4MBytes of RAM
- 60MByte hard disk
- 1.44MByte (3.5") floppy drive
- Enhanced PC keyboard with 12 function keys
- NEC MultiSync 4D VGA color monitor and card
- Transport Card for server-console communications (NGC's token ring or Ethernet NIC)
- Transport protocol software
- Compaq DOS 4.01
- SniffMaster console software installed at the factory.

Transport Card and Transport Protocol Combinations

The turnkey version of the SniffMaster console comes configured to your requirements. On the other hand, the board-and-software version may require some additional configuration, described in "Setting up the SniffMaster Console" on page 3–3. In either case, each console uses one of four possible configurations of Transport Card and transport protocol. The table in Figure 2–1 shows the four possible SniffMaster console configurations for Transport Card and transport protocol.

Transport Card	Transport Protocol
Ethernet: InterLan NI5210	Novell IPX
Ethernet: InterLan NI5210	TCP/IP
Token ring 16/4	Novell IPX
Token ring 16/4	IBM NetBEUI

Figure 2–1. Transport Card and transport protocol combinations for the SniffMaster console.

A console can attach to either an Ethernet or a token ring. All the servers and consoles in your Distributed Sniffer System must have the same transport protocol to communicate with each other.

Front Panel

The SniffMaster turnkey console comes equipped with a floppy drive, various light-emitting diode (LED) indicators, and a power switch on the front panel. You can see them in Figure 2–2.

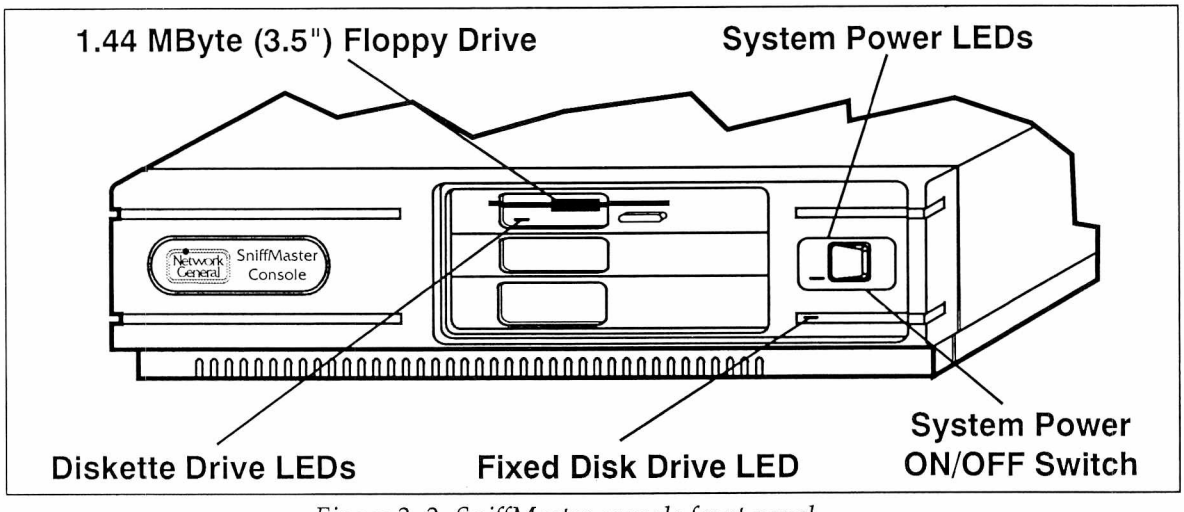


Figure 2–2. SniffMaster console front panel.

Floppy Drive	Accommodates 1.44 (3.5") floppy disks.
System Power LED	Green LED lights when system unit is turned on.
Diskette Drive LED	Color of the LED identifies the type of operation: *green* when a high-density diskette is accessed and *orange* when a low-density diskette is accessed.
Fixed Disk Drive LED	Green indicator when the fixed disk is accessed.

System Power Switch	Push on right side to turn on; push to left side to turn off.

Back Panel

The SniffMaster turnkey console comes equipped with several interface connectors on the back panel. You can see them in Figure 2–3.

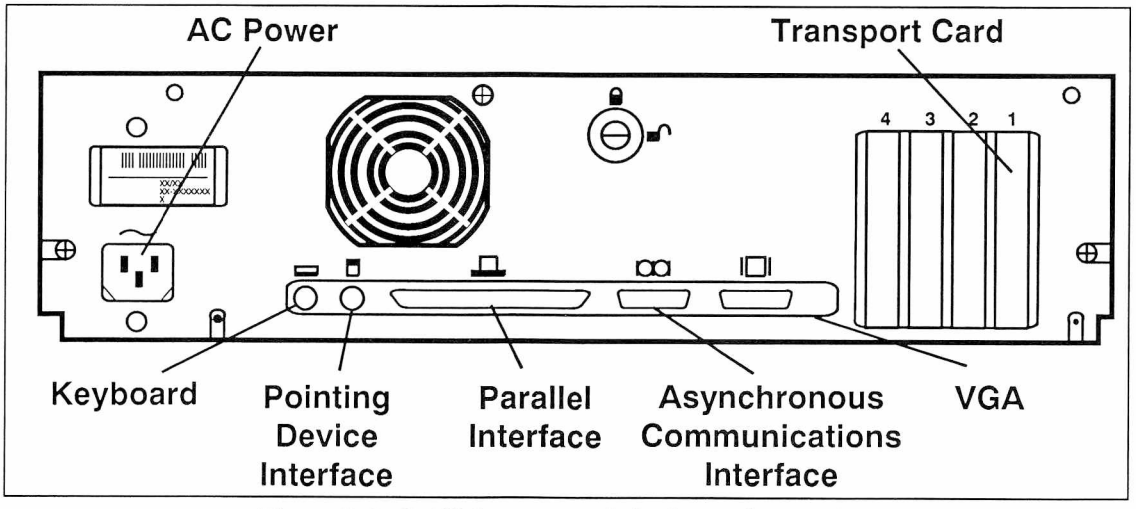


Figure 2–3. SniffMaster console back panel controls.

AC Power	Used for connecting the power cord.
Keyboard	Used for connecting the keyboard cable.
Pointing Device	Used for connecting a pointing device (mouse) interface.
Parallel	Used for connecting devices such as a printer or a plotter.
Asynchronous Communications	COM port 1. Used for connecting serial devices such as modems, printers, and plotters.
VGA	Used for connecting a VGA-compatible monitor.
Transport Card	Used for connecting to an Ethernet or token ring network and to communicate with Sniffer servers.

Sniffer Server

Three combinations of applications software are available on Sniffer servers:

- Monitoring-only
- Analysis-and-monitoring
- Analysis-only.

All servers are available only as turnkey systems. They come with various combinations of NICs and transport protocols.

Components

Sniffer servers come equipped with the following hardware and software components:

- Server chassis with power supply.
- Intel 80386sx microprocessor.
- 1MByte of RAM for monitoring-only servers; 5MByte of RAM for analysis and monitoring servers and for analysis-only servers.
- 40MByte hard disk.
- Two serial interface ports: COM1 and COM2.
- Parallel interface port: LPT1.
- Sniffer monitoring or analysis applications software installed at the factory.
- Two ISA bus 16-bit interface card slots.
- Two NICs. One is the Transport Card for server-console communications; the other is the Monitor Card for monitoring and/or analyzing.
- Transport protocol software.

Configurations

The two major configuration dimensions for servers are network type and transport protocol. *Monitoring-only* and *analysis-and-monitoring* servers can observe either Ethernet or token ring. Communication with consoles must be over the same network type. *Analysis-only* servers can analyze WAN traffic and use either Ethernet or token ring to communicate with consoles. All the servers and consoles in your Distributed Sniffer System that you want to communicate with one another must have the same transport protocol.

The table in Figure 2–4 shows the four possible configurations for the *monitoring-only* server.

Monitor Card	Transport Card	Transport Protocol
Ethernet: InterLan NI5210	Ethernet: InterLan NI5210	Novell IPX
Ethernet: InterLan NI5210	Ethernet: InterLan NI5210	TCP/IP
Token ring 16/4	Token ring 16/4	Novell IPX
Token ring 16/4	Token ring 16/4	IBM NetBEUI

Figure 2–4. NIC and transport protocol combinations for the monitoring-only Sniffer server.

The table in Figure 2–5 shows the four possible Sniffer *analysis-and-monitoring* server configurations.

Monitor Card	Transport Card	Transport Protocol
Ethernet: 3Com 3C505	Ethernet: InterLan NI5210	Novell IPX
Ethernet: 3Com 3C505	Ethernet: InterLan NI5210	TCP/IP
Token ring 16/4	Token ring 16/4	Novell IPX
Token ring 16/4	Token ring 16/4	IBM NetBEUI

Figure 2–5. NIC and transport protocol combinations for the Sniffer analysis-and-monitoring server.

The table in Figure 2–6 shows the four possible Sniffer *analysis-only* server configurations.

Monitor Card	Transport Card	Transport Protocol
WAN	Ethernet: InterLan NI5210	Novell IPX
WAN	Ethernet: InterLan NI5210	TCP/IP
WAN	Token ring 16/4	Novell IPX
WAN	Token ring 16/4	IBM NetBEUI

Figure 2–6. NIC and transport protocol combinations for the Sniffer analysis-only server.

Front Panel

Sniffer servers come equipped with several LED indicator lights and a switch on the front panel. You can see them in Figure 2–7.

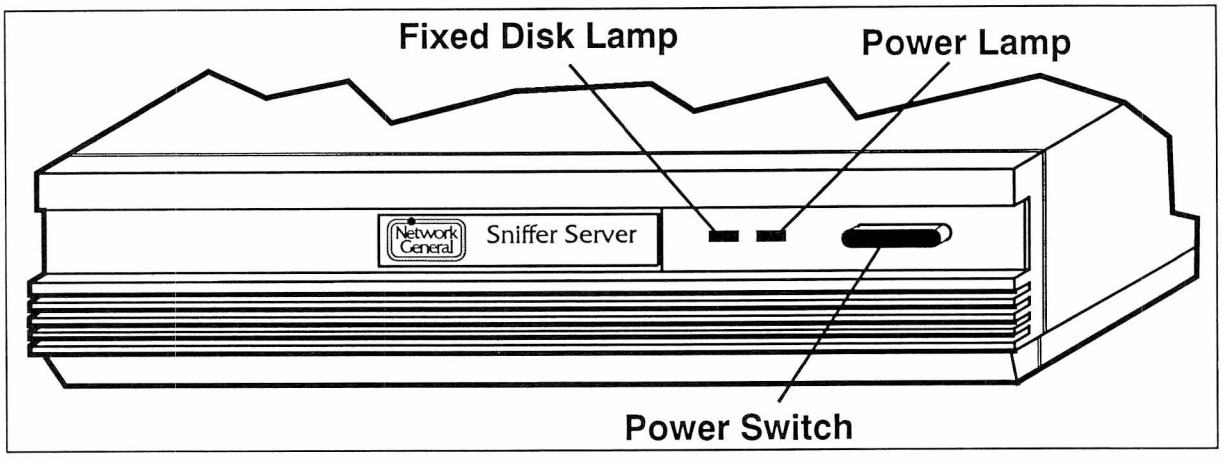


Figure 2–7. Sniffer server front panel.

Fixed Disk Lamp	Indicates that hard disk is being accessed.
Power Lamp	Green indicates operation with higher processor speed. Red indicates slower processor speed.
Power Switch	Push once to switch on. Push again to switch off.

Back Panel

Sniffer servers come equipped with several controls and connectors on the back panel. You can see them in Figure 2–8.

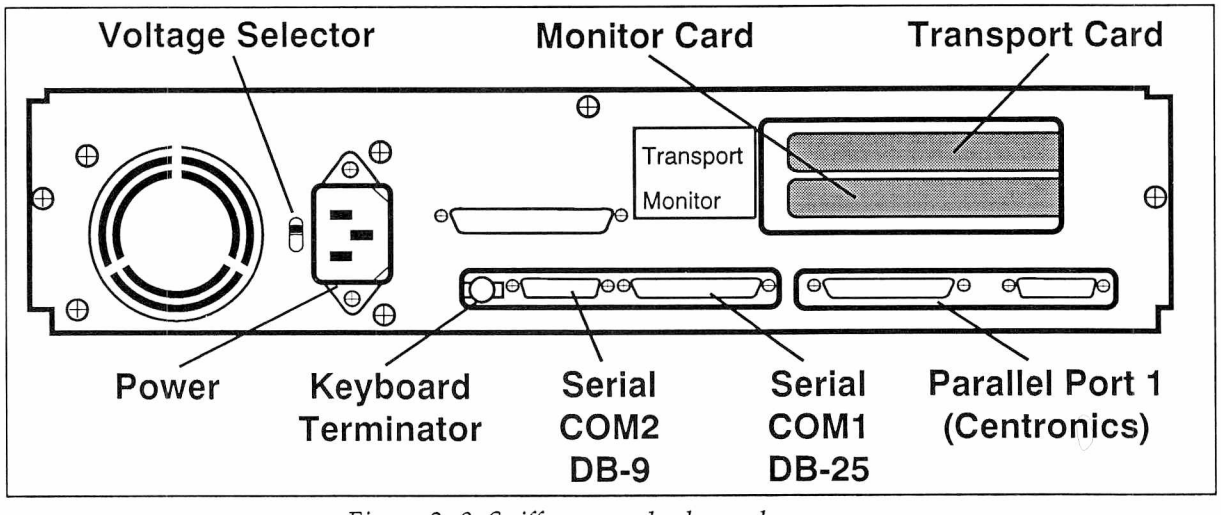


Figure 2–8. Sniffer server back panel.

Transport Card	NIC used for communicating with the SniffMaster console.
Monitor Card	NIC used for observing traffic on, and capturing traces from, a network.
Voltage Selector	Set correctly for the local electrical supply: 115, nominal voltages 100 to 125 Vac (standard for U.S.); 230, nominal voltages 220 to 240 Vac.
AC Power	Use to connect the AC power cord to the system unit.
Keyboard Terminator	You must put this in place after receiving the unit. Always keep the keyboard terminator in place. The server will not function properly without it.
Serial Connectors	Two serial connectors: one DB-9 for COM port 2 and one DB-25 for COM port 1. Use to connect the signal cable of a serial printer or any other RS-232 device.
Parallel Port	Connector for parallel port 1. Use to connect the signal cable of a parallel printer or any other parallel (Centronics) device.

Documentation

In addition to the manual you're now reading, the following publications will also help you get the most from the Distributed Sniffer System:

- *Distributed Sniffer System: Analyzer Operations Manual*
- *Distributed Sniffer System: Token Ring Monitor Operations Manual*
- *Distributed Sniffer System: Ethernet Monitor Operations Manual*

If you have the turnkey version of the SniffMaster console, you will also have the following publications available:

- *COMPAQ DOS Manual*
- *COMPAQ DeskPro 386/25e Operations Guide*
- *BASIC Reference Manual*

If you have the board-and-software version of the SniffMaster console, you will also have the following publications available:

- *NI5210 Installation Manual*

- *Local Area Network Support Program, User's Guide*

Protecting Your System

This section explains precautions you should take, including back up and restoration procedures. Read this section before using your system. You can easily protect yourself from a disaster by preparing a few diskettes in advance.

- When setting up the turnkey version of the SniffMaster console for the first time, back up everything on it's hard disk to diskettes.
- Once you install and configure either the turnkey or the board-and-software version of the SniffMaster console, periodically back up everything on its hard disk or at least do an incremental backup.
- Remember to transfer periodically certain vital files on each Sniffer server to a SniffMaster console hard disk. Some of these files are identical on all servers of the same type, and some are different:

  Files in the root directories of all servers:

  CONFIG.SYS
  AUTOEXEC.BAT

  Files in the *xx*SNIFF directories of all servers (in this case, *xx* can be either EN or TR):

  STARTUP.*xx*D
  STARTUP.*xx*I
  STARTUP.*xx*S

  Files in the IPXEN directory of an Ethernet server or the IPXTR directory of a token ring server using Novell's IPX transport protocol:

  SHELL.CFG

  Files in the WINTCP directory of an Ethernet server using the TCP/IP transport protocol:

  WINTCP.SYS
  SNMP_NGC.CFG

You will use the DOS utility, BACKUP, for some of these procedures. The first time you run BACKUP, it's probably useful to back up everything. Later, you can back up only those files that are new or have been modified since the last back up (an incremental backup).

The BACKUP utility creates specially formatted files that are not usable until restored with the RESTORE utility.

For further details on the BACKUP utility, you should consult the DOS manual that came with your system.

Backup and Restore Procedures

This section describes procedures that help you protect your system. The procedures describe how you:

- Back up an entire hard disk
- Update the backup of a hard disk
- Limit a backup to a particular directory
- Restore a backup to the hard disk
- Copy vital files from a server to the hard disk of a console.

Follow the procedures below to ensure the safety of your software and data:

To back up the entire hard disk of the SniffMaster console:

1. The backup program formats diskettes during the backup process. However, make sure that you have enough diskettes on hand before you begin. The number of diskettes required to back up your system will vary depending on the number of files you have stored on the hard disk.

   Note: The console must be configured (i.e., if IP address was not configured at the factory) and named before the backup procedure can occur. Do you have a turnkey or a board-and-software version of the console?

   a. If turnkey, see "Turnkey Version" on page 3–3.

   b. If board-and-software, see "Board-and-Software Version" on page 3–6.

2. The following equation will help you estimate the number of diskettes needed to perform a backup:

   Hard disk space in use / Diskette capacity = number of diskettes

   Note: If 7.5 MB is in use on your console and you are backing up to 1.44MByte diskettes, divide 7.5 by 1.4 to get 5.3 (7.5 / 1.4 = 5.3). Since the quotient is more than 5, you need at least 6 diskettes to back up your SniffMaster console.

3. Turn on the console.

   Result: The console software is loaded, and its Main Menu appears if the IP address has been specified and the console named.

4. Use the Cursor keys to highlight **Exit**, and press Enter.

Result: Look for the DOS prompt C:\>.

5. Type the following DOS command:

   BACKUP C:*.* A: /S

   Note: The parameter A: indicates that A is the destination drive. The parameter /S tells DOS to include all files in the directory and all files in any subdirectories of the directory.

6. Press Enter.

7. After the first disk, supply disks to the SniffMaster console as BACKUP prompts. You will be prompted until the entire job is finished. During BACKUP a file may be split so that it starts on one diskette and concludes on another.

8. Label each diskette with a sequence number to keep them in order.

   Note: You may want to indicate on the disk label or in your sequence numbers that this is a full backup. For example, your numbers might be F-1, F-2, F-3, and so on.

To make an incremental (update) backup:

1. Make certain you have enough diskettes on hand before you begin.

2. Type the following DOS command.

   BACKUP C:*.* A: /S/M

   Note: The parameter /S tells DOS to include all files in the directory and all files in any subdirectories of the directory. The parameter /M means "modified," that is, only files that are new or have changed since your last backup will be copied.

3. Press Enter.

   Result: Look for the message,

   ```
   Files in the target drive A:\ root directory will be erased. Press any key
   to continue.
   ```

4. Insert the first disk, and press any key.

5. After the first disk, supply disks to the SniffMaster console as BACKUP prompts. You will be prompted until the entire job is finished. During BACKUP a file may be split so that it starts on one diskette and concludes on another.

6. Label each diskette with a sequence number to keep them in order.

   Note: You may want to indicate on the disk label or in your sequence numbers that this is an incremental backup. For

example, your numbers might be I-1, I-2, I-3, and so on.

To limit a backup to a particular directory:

Type the following command at the DOS prompt:

BACKUP C:\[*DIRECTORYNAME*]*.* A:

Note: You may, for example, store files saved from the capture buffers of various analysis servers in a particular directory named CAPTURE. You would then type:

BACKUP C:\CAPTURE*.* A:

To restore files from a backup to the hard disk if the hard disk is functioning and has DOS installed on it:

1. Exit all applications, and return to the DOS prompt C:\>.
2. At the DOS prompt, type a RESTORE command like the following:

   RESTORE A: C:*.* /S

   Note: Here, as with BACKUP, the parameter /S indicates that you want all files in the directory as well as its subdirectories.
3. Press Enter.
4. Insert the first backup disk when the system prompts you.

You can elect to restore only files in a particular directory, particular files, or files that were modified since the date you ran the back up.

In the event that you can't run DOS on the hard disk (for example, because you've reformatted it without including the system files), boot the SniffMaster console from the DOS diskette supplied with your PC. To prepare the hard disk for loading DOS onto it, you must use both the FORMAT and the FDISK commands. Then type the RESTORE command as shown above.

To back up critical files on an installed, configured, and connected Sniffer server:

1. On the console, create a set of directories in advance in which to store the files you will back up from each server. You may want to have one directory per server.
2. Load the File Transfer Utility (see "To set up a server and the console to transfer files:" on page 4–34).
3. Use the **Transfer file to console** option on the Miscellaneous Controls menu ("To transfer a file from a Sniffer server to the SniffMaster console:" on page 4–35).
4. Repeat for each file to be transferred.

CHAPTER THREE: INSTALLATION AND CONFIGURATION 3

Network General

Chapter 3. Installation and Configuration

Chapter Overview

This chapter explains how to configure the SniffMaster console and Sniffer servers and how to attach them to your networks.

Installation and configuration of the Distributed Sniffer System is a three-stage process:

- **Setting Up the SniffMaster Console.** The number of steps will vary depending upon whether you have the turnkey version or the board-and-software version.
- **Setting Up the Sniffer Servers.** You set up servers by configuring the transport protocol, if necessary; connecting them to their respective networks; and verifying that they start up correctly.
- **Configuring Sniffer Servers.** You configure servers by establishing connections with each of the servers and using the server configuration utility.

Setting up the SniffMaster Console

The first stage of installation and configuration involves setting up the SniffMaster console, the device used to control the Sniffer servers.

The procedure you will use depends upon which version of the SniffMaster console you have: the turnkey version or the board-and-software version. The most important difference between the setup procedures is that with the board-and-software version, you supply your own PC and must install the board and software yourself.

Turnkey Version

The installation of the turnkey version of the console has just a few steps:

- **Assemble SniffMaster Console.** Use the manual that accompanies the console for instructions.
- **Connect the Transport Card.** The Transport Card is dedicated to communicating with Sniffer servers. Each Sniffer server also has a Transport Card for communications.
- **Configure Transport Protocol (TCP/IP only).** The SniffMaster Console Initialization Program lets you enter the IP address, the subnet mask, and the default IP gateway address.

- **Name the Console.** One other step is to name the console. Giving a name to the SniffMaster console is especially useful if you plan to have more than one console in your Distributed Sniffer System. The name will appear in the left-hand panel of the SniffMaster Main Menu.

  The name you give at this point can have another, more important purpose when using NetBIOS. When a user of another console attempts to log onto a server configured for just one console and one console is already logged on, that user will be given the name of the console already logged onto that server.

  The name will be stored in the STARTUP.SNM file in the CONSOLE directory. If you ever want to change it, you'll need to modify that file with the DOS line editor, EDLIN, or with some other text editor.

To set up the turnkey version of the SniffMaster console:

1. Assemble the turnkey version of the console according to the instructions in *COMPAQ DeskPro 386/25e Operations Guide.*
2. Check the configuration sheet that accompanied your console. Is the Transport Card configured correctly for your type of network?
   - If token ring, the card data rate will be preconfigured for either 16Mbps or 4Mbps. However, if this isn't correct, you can find instructions for changing the configuration in "16/4 Token Ring Network Interface Card" on page 3–37.

     A mismatch of data rate setting on the token ring card with the data rate of the network will bring down your network.

   - If Ethernet, the card will be preconfigured for either "Thick Ethernet" or "Thin Ethernet." However, if this isn't correct, you can find instructions for changing the configuration in "Thick or Thin Ethernet" on page 3–40.
3. Connect the console's Transport Card to the network. Do you have token ring or Ethernet?
   - If token ring, you can see the token ring connector in Figure 3–26.
   - If Ethernet, you can see the Ethernet connectors in Figure 3–27. Furthermore, if you have an Ethernet transceiver cable that is designed for lockposts, you may need an adapter plate to secure it to the server's Transport Card. Instructions for this are in "Securing an Ethernet DB-15 Connector to the Unit" on page 3–44.
4. Power on the console.

5. Are you using TCP/IP as your transport protocol?
   - If yes, see "SniffMaster Console" on page 3–27.
   - If no, go on to the next step.
6. When you see a window (Figure 3–1) prompting you to name the station during the initialization of the SniffMaster console, type in the name of the console.

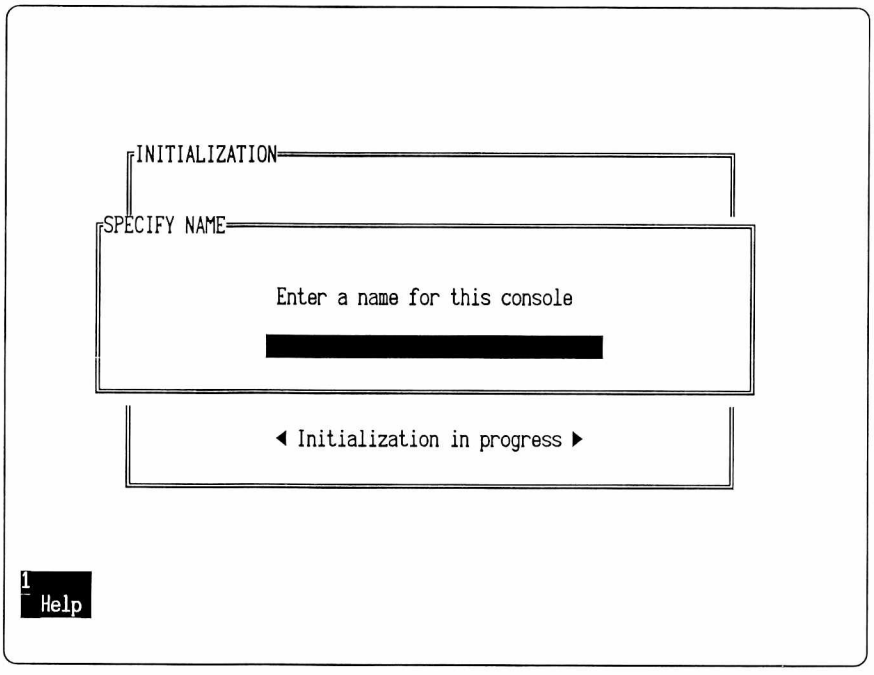


Figure 3–1. Specify Name window for naming a SniffMaster console.

7. Record the console name in your Distributed Sniffer System records. See Appendix C., "System Configuration Record."
8. Press Enter.

   Result: The SniffMaster console's initialization screen appears.
9. Press any key.

   Result: The SniffMaster console's Main Menu appears (Figure 4–1).
10. You are now ready to set up your Sniffer servers. Go now to the section, "Setting up the Sniffer Server" on page 3–11.

    Note: For more information on operating the SniffMaster console, see Chapter 4., "Operation of the Distributed Sniffer System."

    Result: The SniffMaster console's Main Menu appears (Figure 4–1).

Board-and-Software Version

The procedure described in this section applies only to the board-and-software version of the SniffMaster console. This version of the console has several unique installation and configuration steps as well as some that are common to both versions:

- **Check and Install the Transport Card.** The console network interface card is known as the Transport Card in the Distributed Sniffer System. The Transport Card is dedicated to communicating with Sniffer servers. Each Sniffer server also has a Transport Card for communications.

  Before inserting the card in the PC chassis, you must make certain that the Transport Card settings are unique. That is, no other card in your SniffMaster console, or devices attached to your SniffMaster console, can use the same settings. You need not change the settings unless they conflict with other devices.

  If you have a token ring card, you must also check to make sure that the data rate switch on the card matches the data rate of your network.

- **Connect the Transport Card.** The Transport Card is dedicated to communicating with Sniffer servers. Each Sniffer server also has a Transport Card for communications.

- **Install the Console Software.** The Distributed Software Installation Utility installs the console software for you. You will use a special installation utility on the SniffMaster console diskette to install the console software.

  The utility's menu system works exactly the same way as the SniffMaster console menu system. For more information about the basic menu conventions used with the Distributed Sniffer System products, see "Menu Tree" on page 4–4.

- **Configure Transport Protocol (TCP/IP only).** The SniffMaster Console Initialization Program lets you enter the IP address, the subnet mask, and the default IP gateway address.

- **Name the Console.** One other step is to name the console. Giving a name to the SniffMaster console is especially useful if you plan to have more than one console in your Distributed Sniffer System. The name will appear in the left-hand panel of the SniffMaster Main Menu.

  The name you give at this point can have another, more important purpose when using NetBIOS. When a user of another console attempts to log onto a server configured for just one console and one console is already logged on, that user will be given the name of the console already logged onto that server.

The name you enter at this time will be stored in the STARTUP.SNM file in the CONSOLE directory. If you ever want to change it, you'll need to modify that file with the DOS line editor, EDLIN, or with some other text editor.

To set up the board-and-software version of the SniffMaster console:

1. Make certain the PC you intend to dedicate as a SniffMaster console meets the requirements listed in"Board-and-Software Version" on page 3–6.
2. Are there any conflicts between your new console Transport Card the settings of existing cards or other peripherals? If there are conflicting settings, change the appropriate switch or jumper settings:
   - If token ring, see the manual, *Local Area Network Support Program, User's Guide*, for more detailed information on changing the switches. You can find the factory preset switch settings for the token ring card in the table in Figure A–2.
   - If Ethernet, see the manual, *NI5210 Installation Manual*, for more detailed information on changing the jumpers. You can find the factory preset jumper settings for the InterLan card in the table in Figure A–1.

     Note: If you are using TCP/IP as your transport protocol, you have several additional steps after changing the jumpers on the card. You'll also need to change the software to recognize the software:

     a. If necessary, exit to the DOS prompt from the console application.

     b. Change to the directory containing the file, NGCEXEC.BAT. If you installed the console software to the default installation directories, type

        ```
        C:\CD CONSOLE\WINTCP
        ```

     c. Using the DOS line editor, EDLIN, or some other text editor, modify the command line in NGCEXEC.BAT that installs the driver for the InterLan card. The command line will look like this:

        `interl -I:`*x* `-B:`*xxx* `-M:`*xxxx*

        -I: Interrupt Request Level

        -B: I/O Base Address

        -M: Memory Base Address

        An example would be:

```
interl -I:3 -B:31Ø -M:DØØØ
```

The example sets the interrupt to 3, the I/O base to 310 (hex), and the memory base to D000 (hex).

3. Write the SniffMaster console Transport Card and command line values in your Distributed Sniffer System records. See Appendix C., "System Configuration Record."
4. Check the configuration sheet that accompanied your console. Is the Transport Card configured correctly for your type of network?
   - If token ring, the card data rate will be preconfigured for either 16Mbps or 4Mbps. However, if this isn't correct, you can find instructions for changing the configuration in "16/4 Token Ring Network Interface Card" on page 3–37.

     A mismatch of data rate setting on the token ring card with the data rate of the network will bring down your network.
   - If Ethernet, the card will be preconfigured for either "Thick Ethernet" or "Thin Ethernet." However, if this isn't correct, you can find instructions for changing the configuration in "Thick or Thin Ethernet" on page 3–40.
5. Remove the cover of the PC.
6. Insert the card into an empty slot in the PC.
7. Replace the cover.
8. Connect the console's Transport Card to the network. Do you have token ring or Ethernet?
   - If token ring, you can see the token ring connector in Figure 3–26.
   - If Ethernet, you can see the Ethernet connectors in Figure 3–27. Furthermore, if you have an Ethernet transceiver cable that is designed for lockposts, you may need an adapter plate to secure it to the server's Transport Card. Instructions for this are in "Securing an Ethernet DB-15 Connector to the Unit" on page 3–44.
9. Power on the console.
10. Insert the SniffMaster console diskette in a floppy drive.
11. Make that floppy drive the default drive.
12. Type INSTALL at the prompt.
13. Press Enter.

    Result: The initialization screen of the Distributed Software Installation Utility appears.

14. Press any key.

    Result: The Main Menu of the Distributed Software Installation Utility appears with the highlight on **Options** (Figure 3–2).

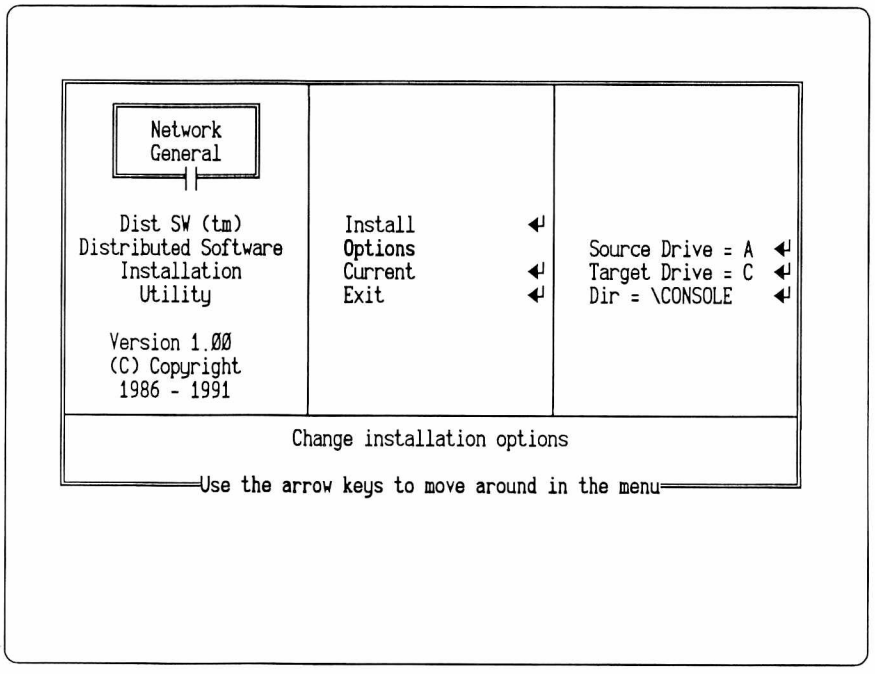


Figure 3–2. Distributed Software Installation Utility Menu.

15. Press the Cursor Right key to move the highlight to the Options menu.

    Note: There are three options in the menu: **Source** specifies the drive from which you want to install the console software, **Target** specifies the drive into which you want to place the console software, and **Dir** specifies the directory that the utility will create and into which the utility will install the console software.

16. Use the Cursor Up or the Cursor Down key to highlight any option you want to change.

17. Press Enter.

18. Type the new specification in the field provided.

19. Press Enter.

20. Repeat the steps above for changes in any of the other options.

21. When you are finished changing the installation options, use the Cursor Left key to move the highlight to the Main Menu.

22. Press the Cursor Up key to highlight **Install** on the Main Menu.

23. Press Enter.

Result: A message appears telling you that the utility is about to install the console software from one drive to another.

24. Press Enter.

    Result: Messages appear telling you the status of the update process.

    The last message to appear gives you a choice as to whether or not you want to update your AUTOEXEC.BAT and/or your CONFIG.SYS files:

    - Press Enter to update.

      If you choose to update, the utility will append SniffMaster console-specific commands to your existing files. It will also save your old files and change the extension by putting a 0 in the last character position of the extension, i.e., .BAT becomes .BA0 and .SYS becomes .SY0, in case you should want to recover their contents. Should you re-install the SniffMaster software, the install utility will automatically save each file with a new extension. The new extension will have the next number in sequence at the last character position of the extension, i.e., .BA1 follows .BA0 and .SY3 follows .SY2.

    - Press Esc to not update.

      If you decide against updating, the utility will leave your files intact. You will need to create special batch files to start the SniffMaster console. You must now create new AUTOEXEC.BAT and/or CONFIG.SYS files. Which one you need to update, or whether you need to update both, depends on the particular network to which you will connect the SniffMaster console and the protocol stack you installed:

      To find out what minimum requirements should be included in the file you create, look at the CONFIG.SWC or AUTOEXEC.SWC files included with the SniffMaster software.

25. Are you using TCP/IP as your transport protocol?

    - If yes, see "SniffMaster Console" on page 3–27.
    - If no, go on to the next step.

26. When you see a window (Figure 3–1) prompting you to name the station during the initialization of the SniffMaster console, type in the name of the console.

27. Record the console name in your Distributed Sniffer System records. See Appendix C., "System Configuration Record."

28. Press Enter.

    Result: The SniffMaster console's initialization screen appears.

29. Press any key.

    Result: The SniffMaster console's Main Menu appears (Figure 4–1).

30. You are now ready to set up your Sniffer servers. Go now to the section, "Setting up the Sniffer Server" on page 3–11.

    Note: For more information on operating the SniffMaster console, see Chapter 4., "Operation of the Distributed Sniffer System."

Setting up the Sniffer Server

This section describes the second stage in setting up your Distributed Sniffer System. So far, you've installed and configured the SniffMaster console. Sniffer servers come almost ready to go. There are a few things you'll need to do to set them up:

- **Attach the Keyboard Terminator.** A keyboard terminator is packed with each server. It looks like a small red thimble. You'll need to insert it into the back of the server. Sniffer servers will not operate correctly without the keyboard terminator.
- **Configure Transport Protocol (TCP/IP only).** You need to do this only if the information was not preconfigured at the factory or if some of the information has changed since the initial configuration. The Sniffer Server Initialization Program lets you enter the IP address. The program lets you enter the IP address, the subnet mask, the default gateway address, and SNMP trap targets.
- **Connect the Transport and Monitor Cards.** Each Sniffer server has two network interface cards (NIC). One NIC, the Transport Card, is for SniffMaster console communications; the other, the Monitor Card, is for observing a network. Sniffer servers can observe and communicate with the SniffMaster console on the same network. Sniffer servers can also observe on one network segment, ring, or link and communicate with the SniffMaster console on another network segment, ring, or link.
- **Check the Server Diagnostics.** Each Sniffer server has a built-in diagnostic program that runs automatically on startup. It uses distinctive beeps to tell you that it is functioning properly.

To set up a Sniffer server:

1. Attach the keyboard terminator to the back of the unit (see Figure 2–8).

   Note: The keyboard terminator looks like a small red thimble. It must be in place for a server to work. It is packed separately to prevent damage to the server.

2. Are you are using TCP/IP as your transport protocol?

   - If yes, see "Sniffer Server" on page 3–29.
   - If no, go on to the next step.

3. Check the configuration sheet that accompanied your server. Are the Transport and Monitor Cards configured correctly for your type of network?

   - If token ring, the card data rate will be preconfigured for either 16Mbps or 4Mbps. However, if this isn't correct, you can find instructions for changing the configuration in "16/4 Token Ring Network Interface Card" on page 3–37.

     A mismatch of data rate setting on the token ring card with the data rate of the network will bring down your network.

   - If Ethernet, the card will be preconfigured for either "Thick Ethernet" or "Thin Ethernet." However, if this isn't correct, you can find instructions for changing the configuration in "Thick or Thin Ethernet" on page 3–40.

4. Connect the server's Transport Card to the network. Do you have token ring or Ethernet?

   - If token ring, you can see the token ring connector in Figure 3–26.
   - If Ethernet, you can see the Ethernet connectors in Figure 3–27. Furthermore, if you have an Ethernet transceiver cable that is designed for lockposts, you may need an adapter plate to secure it to the server's Transport Card. Instructions for this are in "Securing an Ethernet DB-15 Connector to the Unit" on page 3–44.

5. Connect the server's Monitor Card to the network. Do you have token ring, Ethernet, or WAN?

   - If token ring, you can see the token ring connector in Figure 3–26.
   - If Ethernet, you can see the Ethernet connectors in Figure 3–27. Furthermore, if you have an Ethernet transceiver cable that is designed for lockposts, you may need an adapter plate to secure it to the server's Transport Card. Instructions for this are in "Securing an Ethernet DB-15

Connector to the Unit" on page 3–44.

- If WAN, you can see the WAN connector in Figure 3–28. Special instructions for connecting can be found in "WAN Server" on page 3–46.

6. Power on the Sniffer server.
7. Check the built-in server diagnostics to verify that it started up correctly:
   a. Listen for the first beep. This indicates that the hardware POST (Power-On-Self-Test) has been completed successfully.
   b. Listen for a second audible signal, *Checkpoint 1*. This signal consists of one beep and indicates that its operating system environment has been set.
   c. Listen for a third audible signal, *Checkpoint 2*. These two beeps indicate that memory is initialized.
   d. Listen for the fourth audible signal, *Checkpoint 3*. The three beeps indicate that the communications software has been installed.
   e. Listen for the final musical chime. It tells you that the server is ready.

   Note: If the server failed at any of these checkpoints, check the procedures in Appendix A., "Troubleshooting Guide."
8. Continue on with the next section, "Configuring the Sniffer Server."

Configuring the Sniffer Server

This section describes the final stage in setting up your Distributed Sniffer System. By now you've installed and configured the SniffMaster console and have it running with its Main Menu showing on the display. You also have installed and configured the protocol stack (if you use TCP/IP) of several Sniffer servers and have completed checking their built-in diagnostics. The final configuration of servers has just a few steps:

Establish Communications Between Console and Servers. You will do this by entering its transport address at the console. For each server to be configured, you will then put its Main Selection Menu up on the SniffMaster console's display. The complete instructions for establishing connections with servers are in "Controlling Sniffer Servers" on page 4–18. The basic steps for establishing connection are recapitulated in this section.

Use the Server Configuration Utility. The utility's menu system works exactly the same way as the SniffMaster console menu system. For more information about the basic menu conventions used with the Distributed Sniffer System products, see "Menu Tree" on page 4–4.

This utility gives you up to ten options, depending on the type of server, that are listed and described in the table in Figure 3–3.

Option	Function
Redirect LPT2	When *selected*, redirects local server's LPT2 port to the console. At the console, you can specify LPT1, COM1, or a file (see "Printing" on page 4–59). When *deselected*, output goes to LPT2 port.
Auto Start (monitor only)	When *selected*, automatically starts the monitor application upon re-booting. When this option is *deselected*, you must start the monitor application manually.
Display Mode	Chooses video parameter for displaying the server's screen on the SniffMaster console. Default is color. Choose mono, color, plasma, or LCD.
Address (NetBIOS only)	Provides a user-defined NetBIOS address that replaces the default NetBIOS address given at the factory. 16-character maximum. Case and space sensitive. Enter it in the NetBIOS address field of the console's Manage Names dialog box. See the section, "Managing Names" on page 4–13.
Password	Specifies the password to be used when connecting from a SniffMaster console. 16-character maximum. Case and space sensitive. Default password is "ngc".
Consoles	Sets the number of SniffMaster consoles that can simultaneously connect to this server. Default is one console. Choose one or two consoles.
Keepalive	Enables server messages to console indicating that the server is ready for connection. If the console does not receive the "keepalive" message at the specified interval, it knows the connection is lost. Adjust for your particular network. Higher "keepalive" interval recommended for slower networks. Default is 5. The interval can be 5 to 999 seconds.
Timeout	Sets the transport transmission timeout, the amount of time a server will wait before retransmitting a message. Adjust for your particular network. Higher timeouts recommended for slower networks. Default is 5. Enter a value between 1 and 60 seconds.
Delta	Sets the time period between screen updates. Lower deltas make smoother screen updates. Default is 0.5 seconds. Enter a value from 0.1 to 9.9 seconds.
Save	Saves the configuration to the server's hard disk.
Exit	Quits the configurator and displays the Sniffer server's Main Selection Menu.

Figure 3–3. Options available with the Server Configurator utility.

To configure a Sniffer server:

1. On the SniffMaster console Main Menu, highlight the **Manage names** item (Figure 4–5).
2. Press Enter.

   Result: The Manage Names window appears (Figure 4–7).

3. Use the Cursor keys to highlight **<New server>**.
4. Press Enter.

   Result: A field appears for entering a symbolic server name.
5. Type in a symbolic name for the new Sniffer server.

   Note: The name you enter can help you identify or differentiate each server more readily. This symbolic name serves no other purpose in the operation of the Distributed Sniffer System.
6. Press Enter.

   Result: A field appears for entering the transport address of the server (Figure 4–8).
7. Type in the transport address of the new Sniffer server:

   TCP/IP Transport Address. If the TCP/IP transport address was installed at the factory, you can find the address on the configuration sheet accompanying the unit. Otherwise, find the address assigned to that server.

   NetBIOS Transport Address. The address was installed at the factory. You can find the address on the configuration sheet accompanying the unit, or you can derive it from the Transport Card address. See "NetBIOS Over IPX or NetBEUI" on page 3–35.
8. Press Enter.
9. Press the Esc key to exit to the Main Menu.

   Result: The Main Menu appears.
10. Press F2 (**Server List**). See Figure 4–12.
11. Use the Cursor keys to highlight the Sniffer server to which you want to connect.
12. Press F7 (**Connect**), or press Enter.

    Result: The Password window appears.
13. Type the default password: ngc.
14. Press Enter.

    Result: If the connection is successful, the Current Status column of the Server Status display will read "Logged on." If unsuccessful, the column will read "Logged off" or "Lost."

    - If successful, go on to the next step.
    - If not successful, check Appendix A., "Troubleshooting Guide."
15. Press F8 (**Server screen**).

Result: The Sniffer server's Main Selection Menu appears.

16. Use the Cursor keys to highlight **Configure Server** item in the Sniffer server's Main Selection Menu (Figure 3–4).

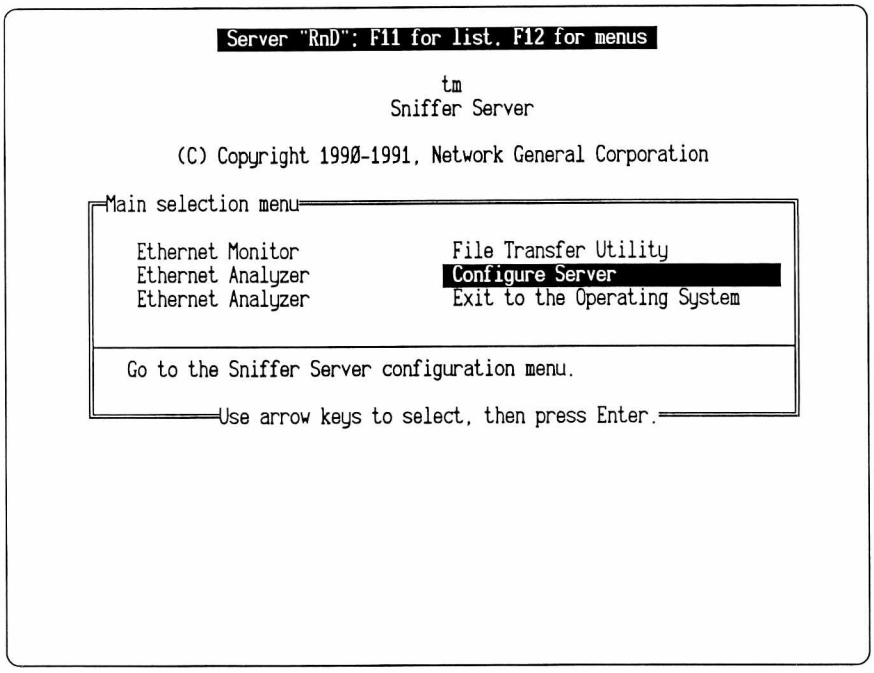


Figure 3–4. Sniffer server Main Selection Menu.

17. Press Enter.

    Result: The result of this action depends on which Sniffer application you have running on your server:

    - If you are configuring a server running just the *analyzer* application, or both the *analyzer* and the *monitor* applications, the Configure Analysis Server menu appears (Figure 3–5).

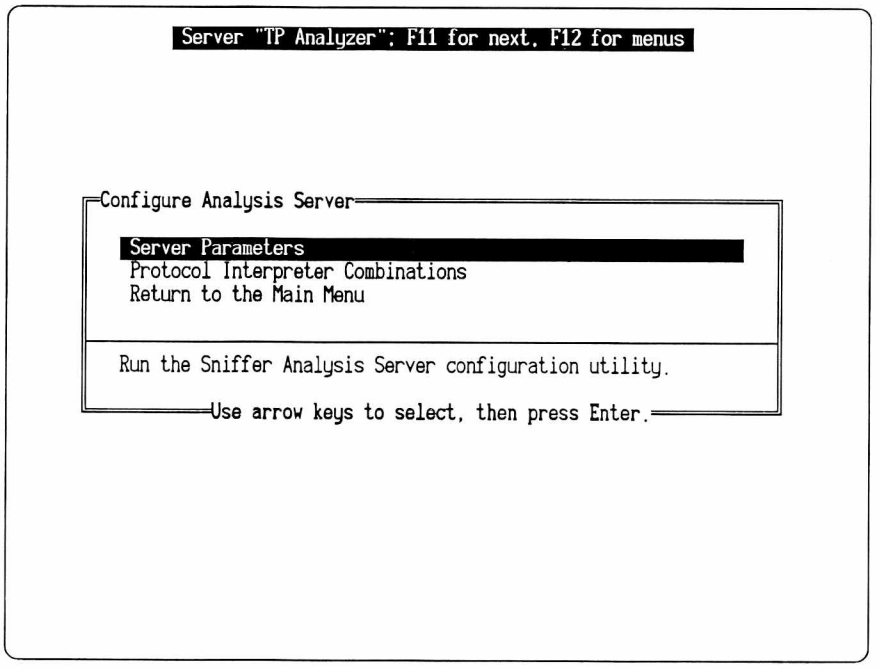


Figure 3–5. Configure Analysis Server menu.

a. Use the Cursor keys to highlight the **Server Parameters** item.

b. Press Enter.

Result: The Server Configurator Main Menu appears (Figure 3–6).

- If you are configuring a server running just the *monitor* application, the Server Configurator Main Menu appears (Figure 3–6).

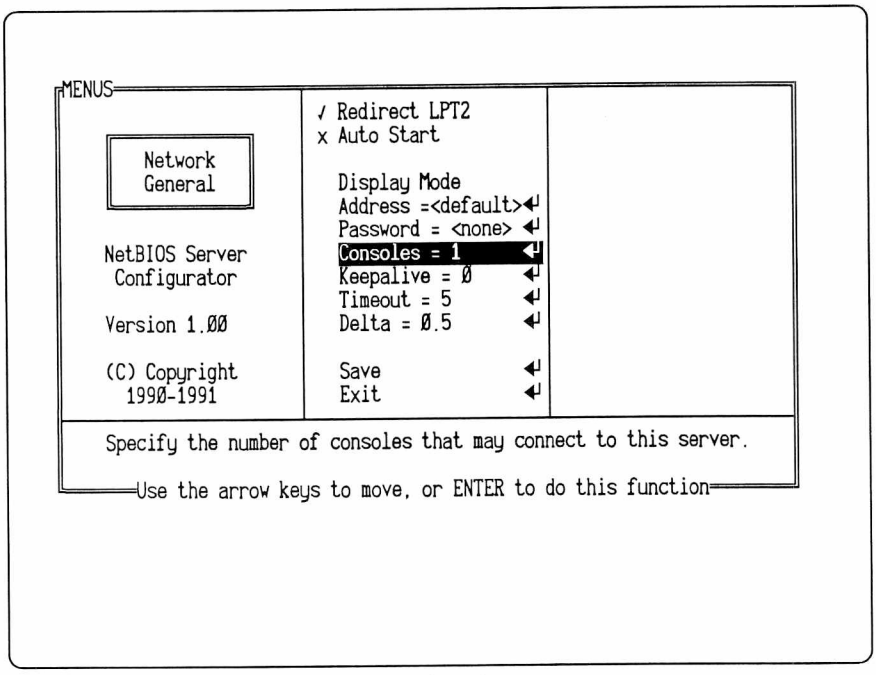


Figure 3–6. Server Configurator Main Menu.

18. Do you want to redirect output to printer port LPT2 to console?
    - If no, skip to the next step.
    - If yes, use the following procedure:
        a. Use the cursor keys to move the highlight to the menu item, **Redirect LPT2.**
        b. Press the Spacebar.

           Result: / means "selected"; x means "deselected."
19. Do you want to start the monitor application (on any non-WAN server) automatically upon re-booting?
    - If no, skip to the next step.
    - If yes, use the following procedure:
        a. Use the cursor keys to move the highlight to the menu item, **Auto Start.**
        b. Press the Spacebar.

           Result: / means "selected"; x means "deselected."
20. Do you want to choose a different type of display screen mode the server will display on the console?
    - If no, skip to the next step.
    - If yes, use the following procedure:

a. Use the Cursor keys to move the highlight to the menu item, **Display Mode**.

b. Use the Cursor Right key to move to the Display Mode menu.

c. Use the Cursor Up or the Cursor Down to highlight the video parameter you want: **Mono, Color, Plasma,** or **LCD**.

d. Press the Spacebar to select.

Result: The pointer moves to indicate your choice.

21. Are you using NetBIOS/NetBEUI or NetBIOS/IPX as your transport protocol?

- If no, skip to the next step.
- If yes, you can specify a substitute address for the default NetBIOS address of the server.

Note: Use only with NetBIOS locally administered addresses:

a. Use the Cursor keys to move the highlight to the menu item, **Address =**.

b. Press Enter.

Result: The Specify Address window opens (Figure 3–7).

c. Type in the address of the NetBIOS server.

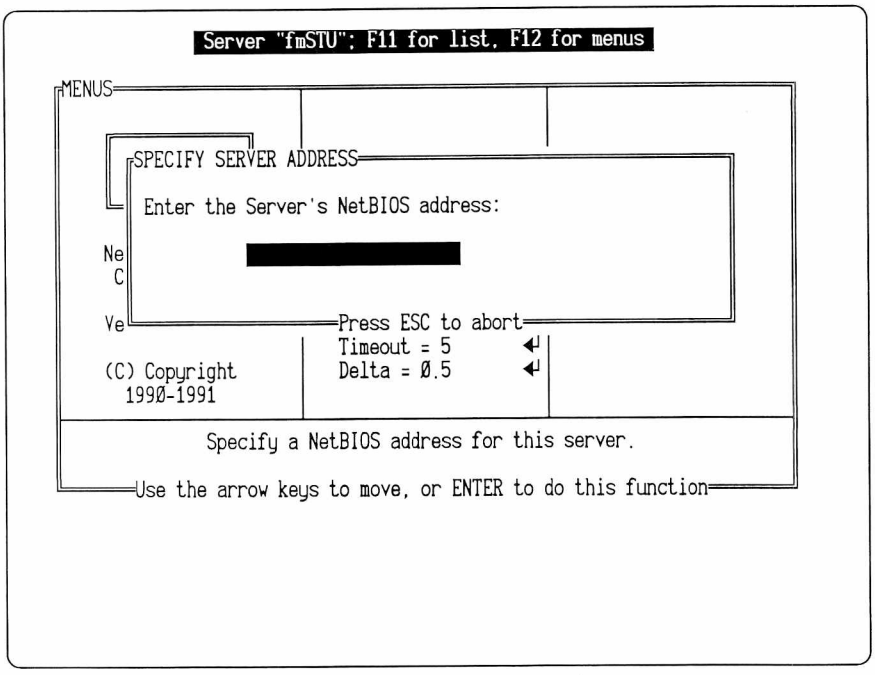


Figure 3–7. Specify Names window for a NetBIOS server.

d. Press Enter.

When you exit the Server Configurator and you opt to put the new configuration into effect, you must remember to record the new transport address you enter here. The address you enter here replaces the default NetBIOS address. If the address gets lost somehow, recovering it is not easy. Record the new address in your Distributed Sniffer System records. See Appendix C., "System Configuration Record." If the address has been lost, see the procedure, "To find the user-defined NetBIOS address and to compare it with the server information entered in the server database:" on page A–14. You must also enter this address in place of the Transport-level address you enter in the **Manage names** item of the SniffMaster console. See the section, "Managing Names" on page 4–13, for more information.

22. The default password for servers is preconfigured at the factory. This secures the unit until you are prepared to enter your own password or to eliminate the password.

The default password is: ngc.

Do you want to change the password for connecting to the Sniffer server?

- If no, skip to the next step.

- If yes, use the following procedure:

  a. Use the cursor keys to move the highlight to the menu item, **Password =**.

  b. Press Enter.

  Result: The Specify Password window opens (Figure 3–7).

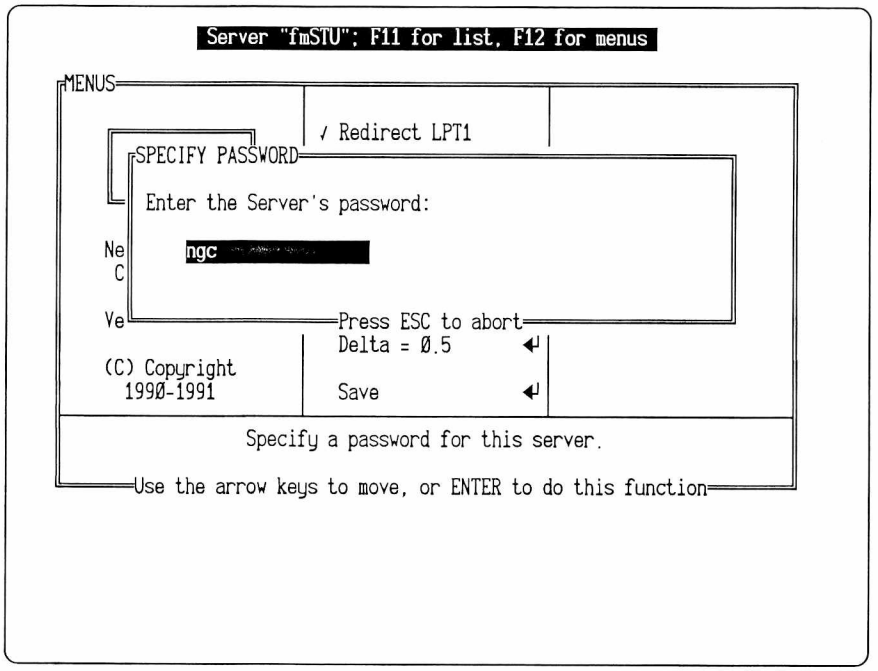


Figure 3–8. Specify Password window.

  c. Use the Backspace key to delete the password in the field.

  Note: If you leave the field blank, the server will require no password when you try to connect to it.

  d. Type in the password that must be entered when someone wants to connect to this Sniffer server from a SniffMaster console.

  Note: Passwords are case-sensitive. Be sure to remember this when connecting to a server.

  e. Press Enter.

23. Do you want to change the number of possible console connections to the Sniffer server?

- If no, skip to the next step.
- If yes, use the following procedure:

a. Use the cursor keys to move the highlight to the menu item, **Consoles =**.

b. Press Enter.

Result: The Specify Console Connections window opens (Figure 3–9).

c. Enter the number of console connections you want to permit.

d. Press Enter.

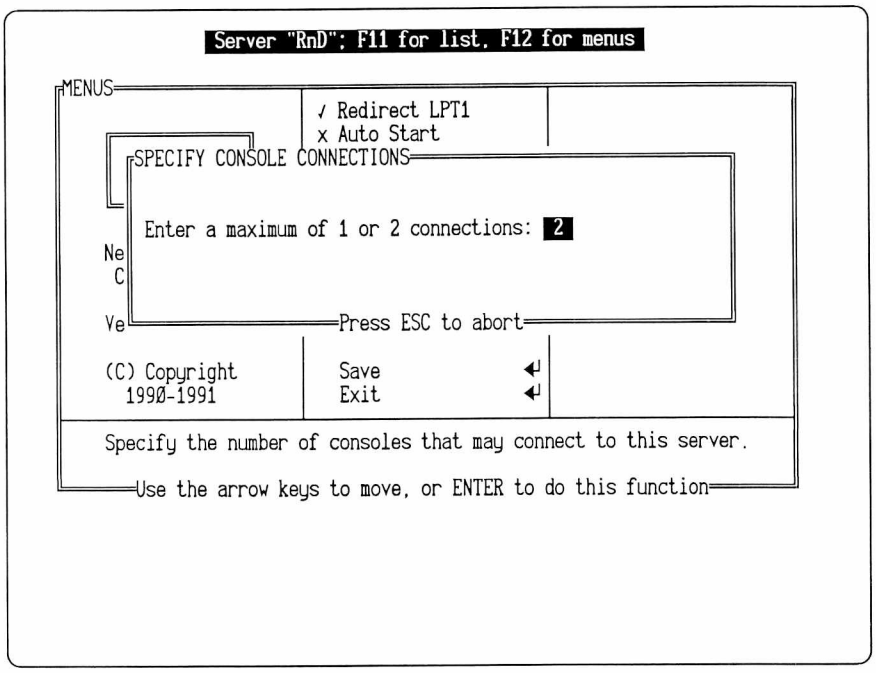


Figure 3–9. Window for specifying the number of SniffMaster consoles that can connect to this Sniffer server.

24. Do you want to change the interval between "keepalive" messages?

- If no, skip to the next step.
- If yes, use the following procedure:

a. Use the Cursor keys to move the highlight to the menu item, **Keepalive**.

b. Press Enter.

Result: The Specify Keepalives window opens (Figure 3–10).

c. Type a value from5 to 999 to indicate the number of seconds between "keepalive" messages.

Note: When you enable "keepalive" messages, the server will tell the console at the interval you specify that it is ready for connection. If the console does not receive a message within the interval, it will assume that the server is inaccessible. The setting you will use depends on your particular network. Use higher values for slower networks.

d. Press Enter.

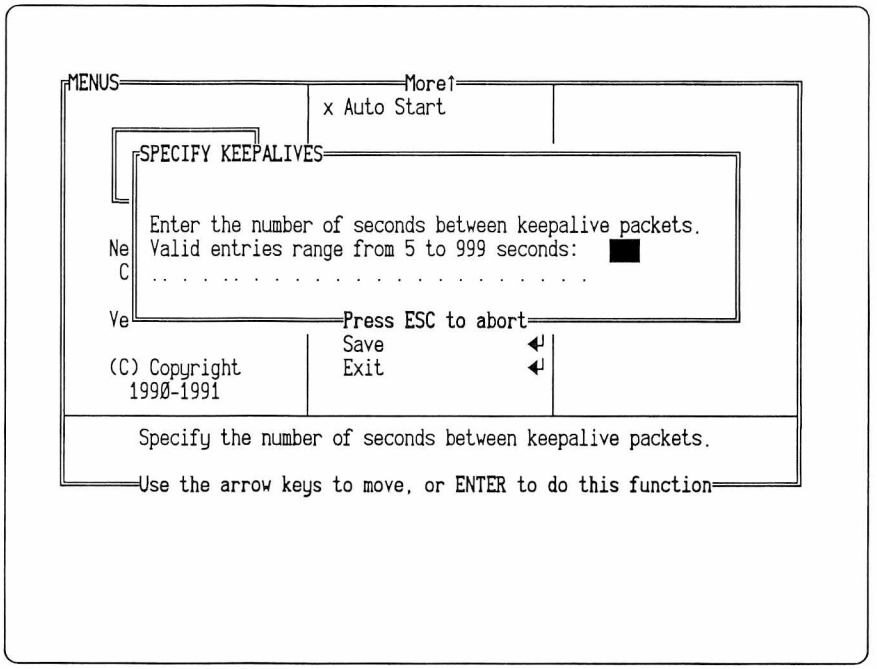


Figure 3–10. Window for specifying the interval between "keepalive" messages from the server.

25. Do you want to change the length of the transport transmission timeout?

    - If no, skip to the next step.
    - If yes, use the following procedure:

      a. Use the Cursor keys to move the highlight to the menu item, **Timeout**.

      b. Press Enter.

      Result: The Specify Transport Timeout window opens (Figure 3–10).

      c. Type a value between 1 to 60 to indicate the number of seconds until a transport transmission timeout.

      Note: The timeout parameter specifies how long the server will wait to receive a reply from a console before

retransmitting a message. The setting you use will depend on the circumstances of your network. Use a higher timeout for slower networks.

d. Press Enter.

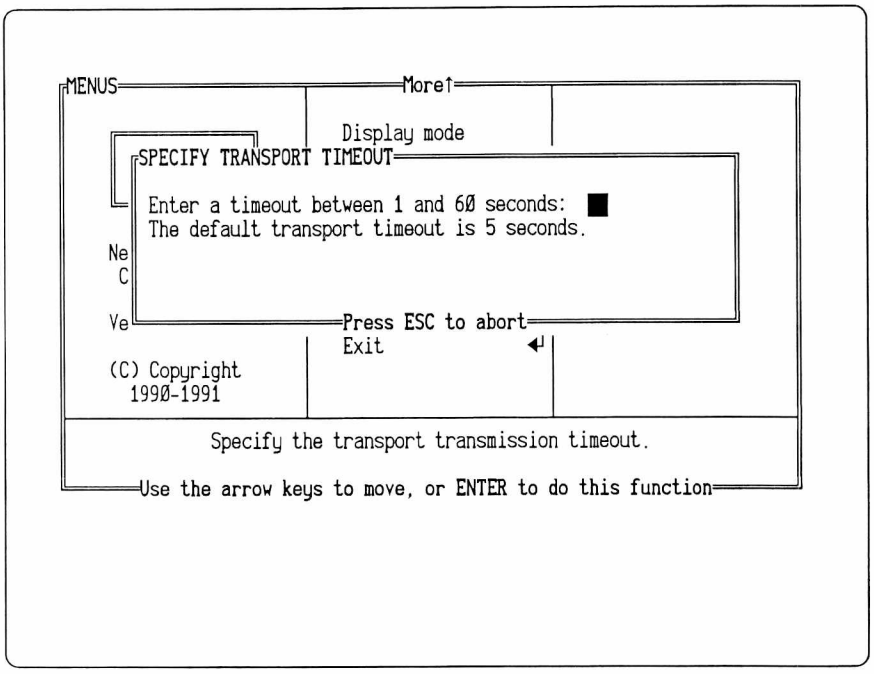


Figure 3–11. Window for specifying the transport timeout.

26. Do you want to change the time period between screen updates?

    - If no, skip to the next step.
    - If yes, use the following procedure:

      a. Use the Cursor keys to move the highlight to the menu item, **Delta**.

      b. Press Enter.

      Result: The Specify Screen Update Period window opens (Figure 3–10).

      c. Type a time period between 0.1 and 9.9 to indicate the number of seconds between screen updates.

      Note: The delta parameter specifies how much time will elapse between screen updates from the server to a console. A small delta will send more screens and use up more bandwidth. A large delta will preserve bandwidth but result in a jerkier display on the console.

      d. Press Enter.

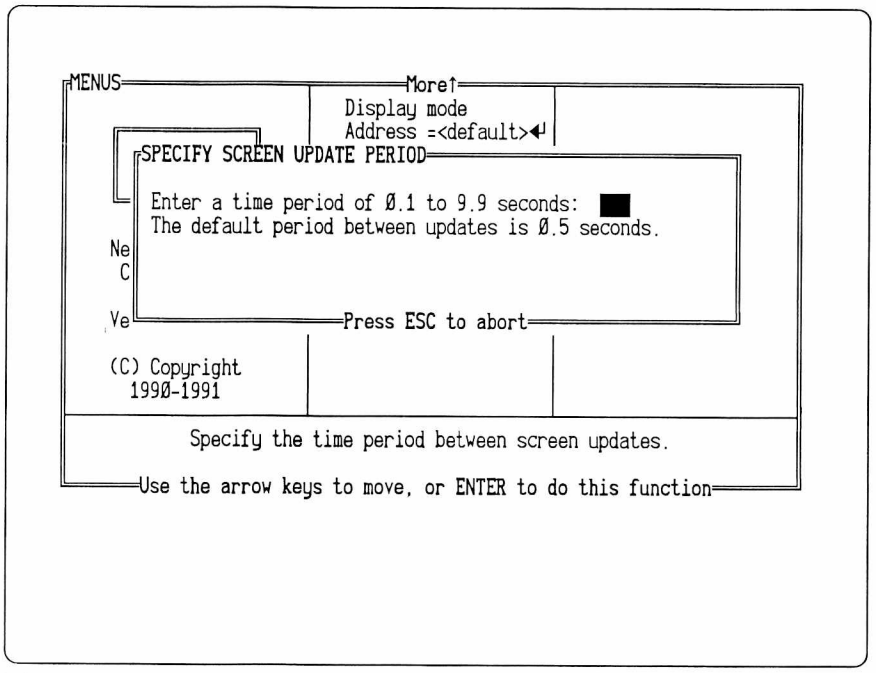


Figure 3–12. Window for specifying the screen update period.

27. Do you want to save the configuration?

    - If no, skip to the next step.

      Note: If you don't save changes to the configuration, you will get a warning when you exit the Server Configurator utility asking if you want to discard any changes. Ignore the warning when you see it.

    - If yes, use the following procedure:

      a. Use the Cursor keys to move the highlight to the menu item, **Save**.

      b. Press Enter.

         Note: A new configuration is saved to special files but takes effect on a server only after you reboot.

28. If you saved the new configuration, do you want it to take effect immediately?

    - If no, use the following procedure:

      a. Use the Cursor keys to highlight **Exit** on the Main Menu.

      b. Press Enter.

         Result: A warning appears asking if you want to reboot the server with the new configuration. Ignore the

warning.

c. Press the Escape key.

Result: The Main Selection Menu of the server appears. If you saved the changes to the configuration, the new configuration is stored in special files until you reboot.

- If yes, use the following procedure:

a. Use the Cursor keys to highlight **Exit** on the Main Menu.

b. Press Enter.

Result: A warning appears asking if you want to reboot the server with the new configuration. You must reboot for the new configuration to take effect.

c. Press the Enter key.

Result: The server reboots, and the connection is lost. If you want to reconnect, you must go back to the Server Status display of the console and press F7 (**Connect**). After reconnecting with the server, the new configuration will be in effect.

Configuring Transport Protocols

In this section, you'll find instructions for configuring the transport protocol installed on your SniffMaster consoles and Sniffer servers. The protocols covered are:

- TCP/IP
- NetBIOS/NetBEUI
- NetBIOS/IPX

Configuring TCP/IP

This section explains how to configure the TCP/IP protocol software. For either a console or a server, you must enter its IP address, IP subnet mask, and IP gateway. For servers only, you can specify SNMP trap targets that let servers direct alarm information to SNMP Network Management Stations.

You will use a console version and a server version of the IP Initialization Program. This utility has two additional uses not described in this section: setting the number of connections to a unit and setting the TCP window size. You can find additional information about, and on the uses of, this program in Appendix B., "Troubleshooting and Fine Tuning Tools and Utilities."

SniffMaster Console

You can configure the SniffMaster console's transport protocol without special equipment or arrangements.

To configure the TCP/IP protocol software on the SniffMaster console:

1. If you haven't already, start the SniffMaster console.

   Result: The IP Initialization Program Menu appears (Figure 3–13).

2. Press any key immediately to use the SniffMaster Console IP Initialization Program Menu.

   Note: When you configure the TCP/IP stack for the first time the IP Initialization Program Menu will appear and pause for you. After the first time, the Menu will always come up when you re-boot the console. You will have five seconds to hit any key to pause. After pausing, you can change the configuration values for a TCP/IP SniffMaster console.

```
Network General IP initialization program.  Version 0.07
(C) Copyright 1991, Network General Corporation
Using wintcp info file C:\CONSOLE\wintcp\wintcp.sys

If you change any settings, this system will optionally reboot when you quit.

       Ipinit commands (and current settings) :
address   - Set IP address            [currently set to 0.0.0.0]
subnet    - Set IP subnet mask        [currently set to 0.0.0.0]
gateway   - Set default IP Gateway    [currently set to 0.0.0.0]
help      - Display this menu
quit      - Exit to DOS
update    - Save changes

Internet address must be set to proceed.

Ipinit>
```

Figure 3–13. SniffMaster Console IP Initialization Program Menu as it appears on the console display.

Figure 3–14 lists three options you can set with the SniffMaster Console IP Initialization Program Menu.

Command	Function
address	Sets the IP address. Use dotted decimal notation to enter the IP address.
subnet	Sets the IP subnet mask. Subnet masks let you partition your network and, thereby, allow a greater number of address assignments. Enter the subnet mask in terms of the number of subnet bits. Typically, this would be a number between 8 and 24. 8 creates a subnet mask of 255.0.0.0. 24 creates a subnet mask of 255.255.255.0.
gateway	Sets the default IP gateway. Use dotted decimal notation to enter the IP address of the default gateway.

Figure 3–14. SniffMaster Console IP Initialization Program Menu options.

3. Type the appropriate Ipinit command for the setting you want to change (e.g., **address, subnet**).

   Note: You can type the entire command or just the first letter.

4. Press Enter.

5. Follow the instructions that appear to change the setting.

6. Record the transport protocol information in your Distributed Sniffer System records. See Appendix C., "System Configuration Record."

7. When you exit the program, you must use the **update** command to save the changes and then reboot the console to install the new configuration:

   a. Type "**u**" to update the changes.

   b. Type "**q**" to quit the program.

   c. When prompted, press any key to confirm intention to quit and to reboot.

8. Are you configuring a turnkey or a board-and-software console?

   - If turnkey version, continue on with Step 6. on page 3–5.
   - If board-and-software version, continue on with Step 26. on page 3–10.

An Example. Figure 3–19 provides an example for changing the address settings on a SniffMaster console with TCP/IP.

```
Network General IP initialization program.  Version Ø.Ø7
(C) Copyright 1991, Network General Corporation
Using wintcp info file C:\CONSOLE\wintcp\wintcp.sys

If you change any settings, this system will optionally reboot when you quit.

       Ipinit commands (and current settings) :
address   - Set IP address            [currently set to Ø.Ø.Ø.Ø]
subnet    - Set IP subnet mask        [currently set to Ø.Ø.Ø.Ø]
gateway   - Set default IP Gateway    [currently set to Ø.Ø.Ø.Ø]
help      - Display this menu
quit      - Exit to DOS
update    - Save changes

Internet address must be set to proceed.

Ipinit> address
Enter an IP address or press Enter to cancel
Example IP address: 192.12.Ø.59
: 192.12.Ø.91
default subnet mask is 255.255.255.Ø (24 bits). Press return if OK, or
 enter new number of subnet bits:
Ipinit> update
Saving changes to NGC console configuration....
System will reset when you quit this program.
Ipinit> quit
Changes saved. Press Esc to abort, any other key to reboot system.
```

Figure 3–15. Example of changing settings on a SniffMaster console with TCP/IP.

At the Ipinit> prompt, we entered the **address** command. The program told us to enter an IP address or to press Enter to cancel the procedure. We were also given an example of an IP address. After entering a new IP address of 192.12.0.91, the program informed us of the default subnet mask and asked if that was acceptable or did we want to enter a new one. We pressed Enter to verify that it was acceptable. When the Ipinit> prompt reappeared, we entered the **update** command and then the **quit** command. Pressing any key will automatically reboot the console.

Sniffer Server

Servers are very powerful and compactly-built computers. To configure TCP/IP protocol software on the server's hard disk, you'll need to attach a terminal or a PC running a terminal emulation program. Then you'll configure the TCP/IP protocol software using the attached terminal.

Included with the SniffMaster console software is the terminal emulation software. You can use this package when using the console to configure TCP/IP on servers.

To attach a PC or terminal to a Sniffer server:

1. Attach one end of a *null modem cable* to the server's COM1 port (Figure 2–8) using the DB-25 connector.

Note: Network General includes a null modem cable with each SniffMaster console. It is a special cable that allows two PCs to be directly connected.

Note: You probably will never have to adjust the COM port parameters for a server. In the event that you do, see "IOFORK.SYS Utility" on page B–11.

2. What are you using as an external terminal to the server?
   - If you're using a SniffMaster console, attach the other end of the cable to the asynchronous communications interface (COM port 1) on a SniffMaster console.
   - If you're using a ASCII terminal, attach the other end of the cable to the serial port on an ASCII terminal.

     Note: The required settings are: 9600 baud, no parity, 8 data bits, and 1 stop bit.
   - If you're using a PC running terminal emulation software, attach the other end of the cable to the COM1 port on a PC running terminal emulation software.
3. Enter terminal emulation mode if you've attached the SniffMaster console or a PC to the server:
   - If you're using the console, follow the steps in the next procedure.
   - If you're using some other terminal emulation software, you'll need to refer to its documentation for specific instructions.

To enter terminal emulation mode using the SniffMaster console:

1. Power on the SniffMaster console.
2. Exit the SniffMaster console software.
3. At the DOS prompt, type CD C:\CONSOLE\R2CALL.
4. Press Enter.
5. At the prompt, type R2CALL.
6. Press Enter.

   Result: The Dialing Directory screen appears (Figure 3–16).

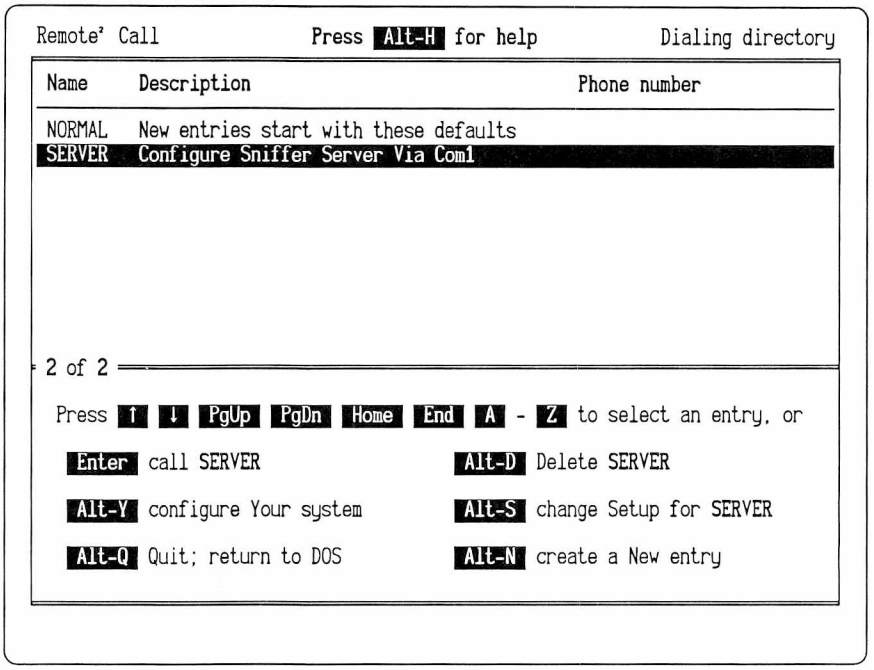


Figure 3–16. The Dialing Directory screen.

7. Press the Cursor Down key to highlight the name SERVER in the extreme left hand column. This is an R2CALL profile that has been pre-configured with the proper settings to communicate with COM1 of the server.

8. Press Enter.

   Result: A blank screen appears. You are now in terminal emulation mode.

To configure the TCP/IP protocol software on a server:

1. Power on the Sniffer server.

   Result: You will hear and see a sequence of diagnostic tones and messages. They will let you know whether or not the server is functioning normally.

2. Check the built-in server diagnostics to verify that it started up correctly:

   a. Listen for the first beep. This indicates that the hardware POST (Power-On-Self-Test) has been completed successfully.

   b. Listen for a second audible signal, *Checkpoint 1*. This signal consists of one beep and indicates that its operating system environment has been set.

   c. Listen for a third audible signal, *Checkpoint 2*. These two

beeps indicate that memory is initialized.

Note: If the server shipped without a IP address, it will stop at the Initialization Program Menu at (Figure 3–17) this point and will not allow you to go any further until you specify an IP address.

Note: After you configure a server and reboot, you will have five seconds to hit any key to pause. Then you can change the configuration values for a TCP/IP Sniffer server.

d. Listen for the fourth audible signal, *Checkpoint* 3. The four beeps indicate that the communications software has been installed.

e. Listen for the final musical chime. It tells you that the server is ready.

Note: If the server failed at any of these checkpoints, check the procedures in Appendix A., "Troubleshooting Guide."

3. If the server was shipped with an IP address, look for the Sniffer server IP Initialization Program Menu on the console screen (Figure 3–17).

Note: The server will pause automatically after the third audible signal if you need to configure the TCP/IP protocol software. After you configure a server and reboot, you will have five seconds to hit any key to pause. Then you can change the configuration values for a TCP/IP Sniffer server.

```
Network General IP initialization program.  Version Ø.Ø7
(C) Copyright 1991, Network General Corporation
Using wintcp info file C:\wintcp\wintcp.sys

If you change any settings, this system will optionally reboot when you quit.

        Ipinit commands (and current settings) :
address   - Set IP address            [currently set to Ø.Ø.Ø.Ø]
subnet    - Set IP subnet mask        [currently set to Ø.Ø.Ø.Ø]
gateway   - Set default IP Gateway    [currently set to Ø.Ø.Ø.Ø]
targets   - Set SNMP trap targets     [currently set to none]
help      - Display this menu
quit      - Exit to DOS
update    - Save changes

Internet address must be set to proceed.

Ipinit>
```

Figure 3–17. Sniffer server IP Initialization Program Menu as it appears on the SniffMaster console running terminal-emulation software.

Figure 3–17 shows a menu that lets you set up to four options with the Sniffer server IP Initialization Program Menu. The table in Figure 3–18 lists and describes the options available on the menu:

Command	Function
address	Sets the IP address.
subnet	Sets the IP subnet mask. Subnet masks let you partition your network and, thereby, allow more address assignments.
gateway	Sets the default IP gateway.
targets	Defines the IP address or addresses to which Simple Network Management Protocol (SNMP) traps generated by this server will be sent. To interpret the SNMP traps at the target Network Management Station, see Chapter 5., "SNMP Network Management Stations in the System."

Figure 3–18. Options on the Sniffer server IP Initialization Program Menu.

4. To change a setting:

   a. Type the first letter of the appropriate command, e.g., "a" for **address**.

   b. Press Enter.

Result: The program will provide you with further instructions and information for changing the setting.

Note: If you ever want to start the IP Initialization Program from the server's DOS prompt, type

```
C:\ipinit -p
```

You will get the standard Sniffer server IP Initialization Program menu that includes options for address, subnet mask, and targets.

5. Write the address, subnet mask, gateway, and targets of each Sniffer server in your Distributed Sniffer System records. See Appendix C., "System Configuration Record."
6. Press "**u**" to **update** changes.
7. Press "**q**" to **quit** the program.
8. Press any key to confirm intention to exit and to reboot.

   Note: You must reboot to install the new configuration.
9. Power off the server.
10. Continue on with Step 3. on page 3–12.

Two Examples. Figure 3–19 provides an example for changing settings on a Sniffer server with TCP/IP.

```
(C) Copyright 1991, Network General Corporation
Using wintcp info file C:CONSOLE\wintcp\wintcp.sys

If you change any settings, this system will optionally reboot when you quit.

       Ipinit commands (and current settings) :
address   - Set IP address            [currently set to Ø.Ø.Ø.Ø]
subnet    - Set IP subnet mask        [currently set to Ø.Ø.Ø.Ø]
gateway   - Set default IP Gateway    [currently set to Ø.Ø.Ø.Ø]
targets   - Set SNMP trap targets     [currently set to none]
help      - Display this menu
quit      - Exit to DOS
update    - Save changes

Internet address must be set to proceed.

Ipinit> address
Enter an IP address or Enter to cancel.
Example IP address: 192.12.Ø.59
: 192.19.Ø.33
default subnet mask is 255.255.255.Ø (24 bits). Press return if OK, or
 enter new number of subnet bits:
Ipinit> update
saving changes to NGC server configuration....
System will reset when you quit this program.
Ipinit> quit
Changes saved. Press Esc to abort, any other key to reboot system.
```

Figure 3–19. Example of changing settings on a Sniffer server with TCP/IP.

At the Ipinit> prompt, we entered the **address** command. The program told us to enter an IP address or to press Enter to cancel the procedure. We were also given an example of an IP address. After entering a new IP address of 192.19.0.33, the program informed us of the default subnet mask and asked if that was acceptable or did we want to enter a new one. We pressed Enter to verify that it was acceptable. When the Ipinit> prompt reappeared, we entered the **update** command and then the **quit** command. The program automatically rebooted the Sniffer server when we pressed any key.

```
address   - Set IP address              [currently set to 192.42.252.91]
subnet    - Set IP subnet mask          [currently set to 255.255.255.0]
gateway   - Set default IP Gateway      [currently set to 192.42.252.32]
targets   - Set SNMP trap targets       [currently set to 2 trap targets]
help      - Display this menu
quit      - Exit to DOS
update    - Save changes
hit any key (within 5 seconds) if you want to change anything: .
Ipinit> targets
Edit trap target list. Current list:
1 - 192.42.252.1.....community name: public
2 - 192.42.252.32.....community name: traps
Options are A(dd), D(elete), Q(uit): a
Enter IP address to add to list: 192.42.252.86
Enter community name for target (or Return for default 'public':
Edit trap target list. Current list:
1 - 192.42.252.1.....community name: public
2 - 192.42.252.32.....community name: traps
3 - 192.42.252.86.....community name: RnD
Options are A(dd), D(elete), Q(uit): q
Ipinit> quit
Save changes before exiting? (y/n)
Saving changes to NGC server configuration...

System will reset when you quit this program.
Changes saved. Press Esc to abort, any other key to reboot system.
```

Figure 3–20. Adding a new SNMP trap target to direct alarm information to a Network Management Station.

Figure 3–20 shows an example of adding an SNMP trap target. As you can see, the Sniffer server was set up for two trap targets when the Sniffer server IP Initialization Program Menu displayed. We entered the command, **targets**, and the program showed the current trap target list. We opted to add a new trap target to the list by entering an "a" at the prompt. The program prompted us first to enter the IP address of the new trap target and then its community name.

NetBIOS Over IPX or NetBEUI

If you use IPX or NetBEUI as your transport protocol, you must follow the procedure in this section to derive the NetBIOS addresses assigned to each server at the factory. You use the NetBIOS addresses when you add each server to the database in the SniffMaster console.

The default NetBIOS addresses are based on hardware addresses. An example would be NGCT786E82. When you use the Configure Server

utility, you can substitute a substitute address for the factory-assigned NetBIOS address to make it easier to remember and to eliminate entry errors. For more information on how you will use them, see the procedure, "To configure a Sniffer server:" on page 3–14.

To derive the NetBIOS address for each Sniffer server:

1. Find the board address label attached to the bottom of the server.

   Note: The board address has 12 hex characters, for example, 10005A786E82 (hex). You will use the last 6 characters of this board address to record the NetBIOS address assigned at the factory.

2. To find the NetBIOS address, replace the first 6 characters of the board address. Do you have token ring or Ethernet?

   - **Token ring.** If you have a token ring board, substitute NGCT for the first 6 characters of the address. Using the address above as an example, you would have a NetBIOS address of NGCT786E82.

   - **Ethernet.** If you have an Ethernet board, substitute NGCE for the first 6 characters of the address. For example, a board with the address, 02070108159c, would have the NetBIOS address, NGCE08159c.

3. If you cannot easily see the address on the label (e.g., on a rack with other machines or in a closet), use the extra label attached to the Sniffer server. Put it where you will be able to see it.

4. Write the NetBIOS address of each Sniffer server in your Distributed Sniffer System records. See "Starting a System Configuration Record" on page C–3.

5. Continue on with Step 7. on page 3–15.

Network Interface Cards

This section covers special procedures you may need to configure and to connect network interface cards. In this section of the chapter, we do not distinguish between Transport Cards and Monitor Cards because the same type of card often serves both purposes.

Configuring Network Interface Cards

You must re-configure a token ring network interface card if you want to change its data rate, e.g., to switch a server's NIC from a 4Mbps token ring to a 16Mbps token ring. Another situation where you must

reconfigure is when you want to switch your Ethernet card from thick to thin Ethernet.

16/4 Token Ring Network Interface Card

The 16/4 token ring adapter card can transmit and capture data over a token ring network at either of two rates: 16 Mbps or 4 Mbps. Make sure you have set the data rate to the appropriate speed before connecting a Sniffer server or SniffMaster console to a token ring network. Connecting a 4 Mbps Sniffer server or SniffMaster console to a 16 Mbps network, or vice versa, will bring down the LAN.

The data rate switch on the adapter card must match the network data rate before you connect the Sniffer server or SniffMaster console. Sniffer servers and SniffMaster consoles usually come from the factory with the data rate switch set to your specification. However, you can use your Sniffer server or SniffMaster console on either a 4 Mbps or 16 Mbps network by changing the data rate switch on the token ring adapter card to match the data rate of the network to which you are connecting.

Each token ring adapter card has one switch block with twelve switches on its component side (Figure 3–21). The twelve switches on the block can easily be moved into the wrong positions. Always handle the card carefully and check each switch to make sure it is in the appropriate position.

The switch settings shown in Figure 3–21 represent no particular configuration.

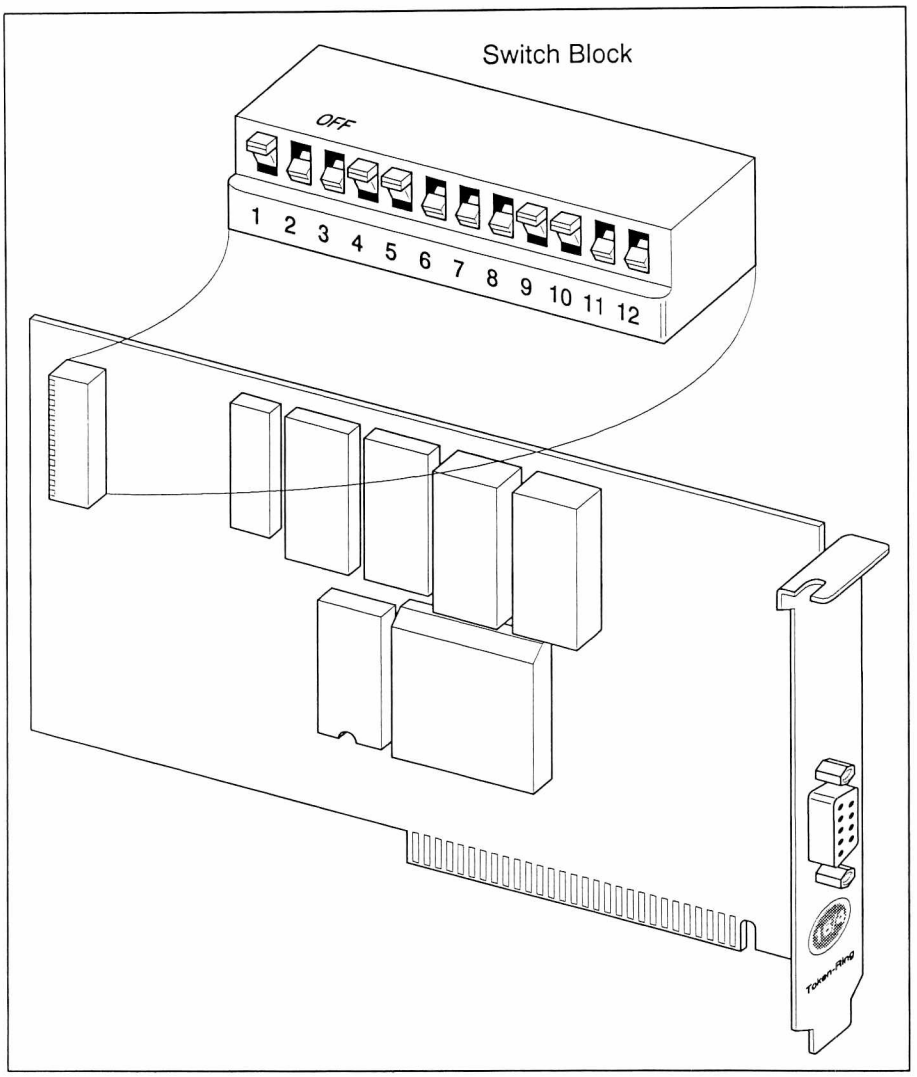


Figure 3–21. Switch block on the token ring card.

The following Figure 3–22, illustrates a switch from this block set in the "off" position.

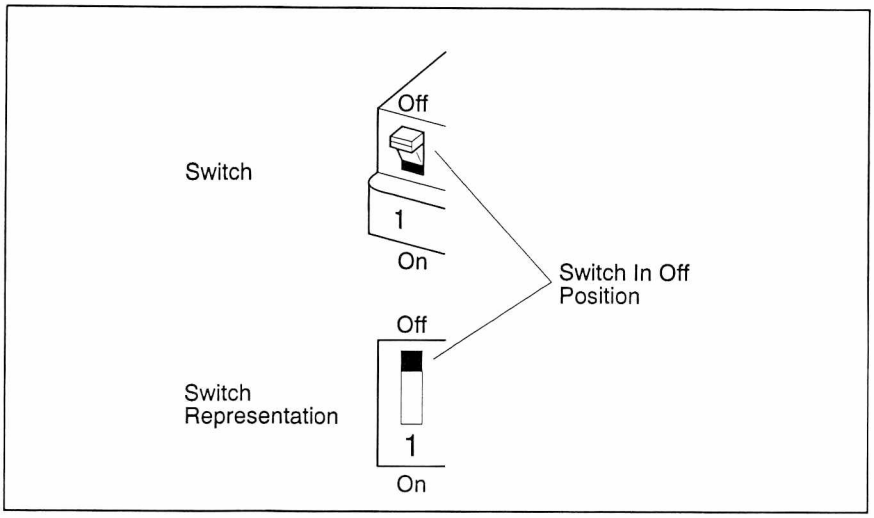


Figure 3–22. Switch in the "off" position.

Switch 12 on the switch block controls the rate at which the adapter will pass data to the network. You can set the adapter data rate to either 16 Mbps or 4 Mbps depending on the network speed.

Below are complete instructions for configuring the card for 16 or 4 Mbps. However, if you need further information on reconfiguring the card, see *Local Area Network Support Program, User's Guide.*

To set the data rate on the token ring NIC:

1. Power down the unit.
2. If necessary, remove the token ring card.
3. Move switch 12 to the "off" position for 16 Mbps or to the "on" position for 4 Mbps.

   Note: Figure 3–22 shows the difference between the "on" and the "off" positions. See also the illustration of switch 12 on the switch block in Figure 3–23 for the correct positions for each data rate.

   Be extremely careful not to move other switches when you move switch 12. The defaults were set at the factory and should not be changed, except possibly in the case of a board-and-software console. You can find the factory settings for the board-and-software console in the table in Figure A–2.

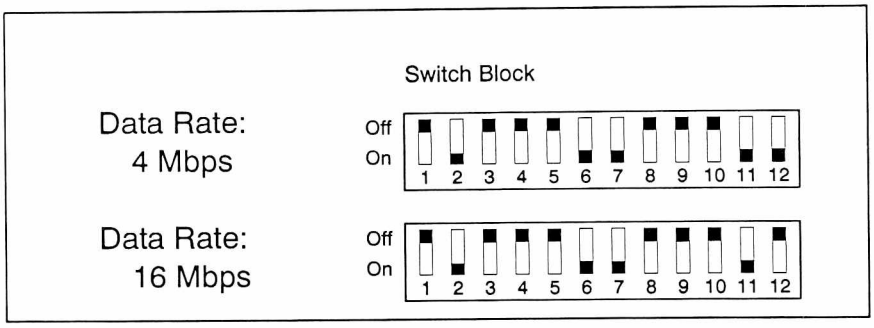


Figure 3–23. Data rate switch positions for switch 12.

Thick or Thin Ethernet

This section describes how to change an Ethernet card to "Thick Ethernet" or "Thin Ethernet."

Your Ethernet card has two connectors (Figure 3–27):

- An AUI (Attachment Unit Interface) or DIX (DEC/Intel/Xerox) DB-15 connector used to attach to an external transceiver for "Thick Ethernet."
- A BNC (bayonet-Neill-Concelman) connector for "Thin Ethernet" that uses the on-board transceiver.

The Distributed Sniffer System utilizes two different Ethernet NICs, depending on the particular needs and parts of your system:

- One is the InterLan NI5210.
- The other is the 3Com 3C505.

Both Ethernet cards come preset for "Thick Ethernet" or "Thin Ethernet," depending upon the configuration you ordered from the factory.

InterLan NI5210 NIC

The transceiver select switch is located on the mounting bracket of the board. The switch is labeled "E" for standard Ethernet and "T" for Thin Ethernet (Figure 3–24).

If your NIC was installed at the factory with the switch in the "E" position, the external transceiver is selected, and you can use the card with "Thick Ethernet." On the other hand, if your NIC was installed with the switch in the "T" position, the on-board transceiver is selected, and you can use the card with "Thin Ethernet."

To reconfigure your card you must change the transceiver select switch from one position to the other.

To reconfigure the InterLan NI5210 NIC:

1. Power down the unit.
2. Locate the transceiver select switch on the mounting bracket of the NI5210 (Figure 3–25). The switch is labeled "E" for standard Ethernet and "T" for Thin Ethernet.
3. Push the switch to the setting you want.
4. Turn the unit on.

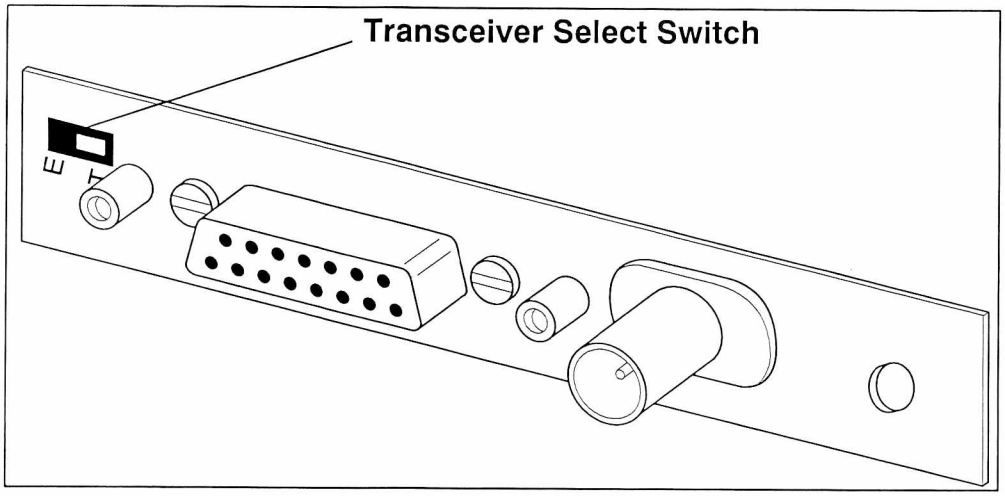


Figure 3–24. Transceiver select switch for the InterLan NI5210 Ethernet NIC.

3Com 3C505 NIC

If your Ethernet card (3Com 3C505) was installed at the factory with the jumper block in theAUI position, the external transceiver is selected, and you can use the card with "Thick Ethernet." If it was installed in the BNC position, the on-board transceiver is selected, and you can use it with "Thin Ethernet."

To change transceivers, you must change the AUI/BNC select jumper from one position to the other.

To reconfigure the 3Com 3C505 NIC:

1. Power down the unit.
2. Remove the Ethernet card.
3. Pull off the AUI/BNC select jumper on the Ethernet card.
4. After you remove the jumper, look for bent or damaged pins.
5. Look for the "BNC" and "AUI" labels on the card. Line up the jumper with the pins associated with the appropriate label.
6. Carefully press the jumper into the new position. Apply even

pressure when you insert the jumper to avoid bending any of the pins.

7. Put the Ethernet card back in the unit.
8. Turn the unit on.

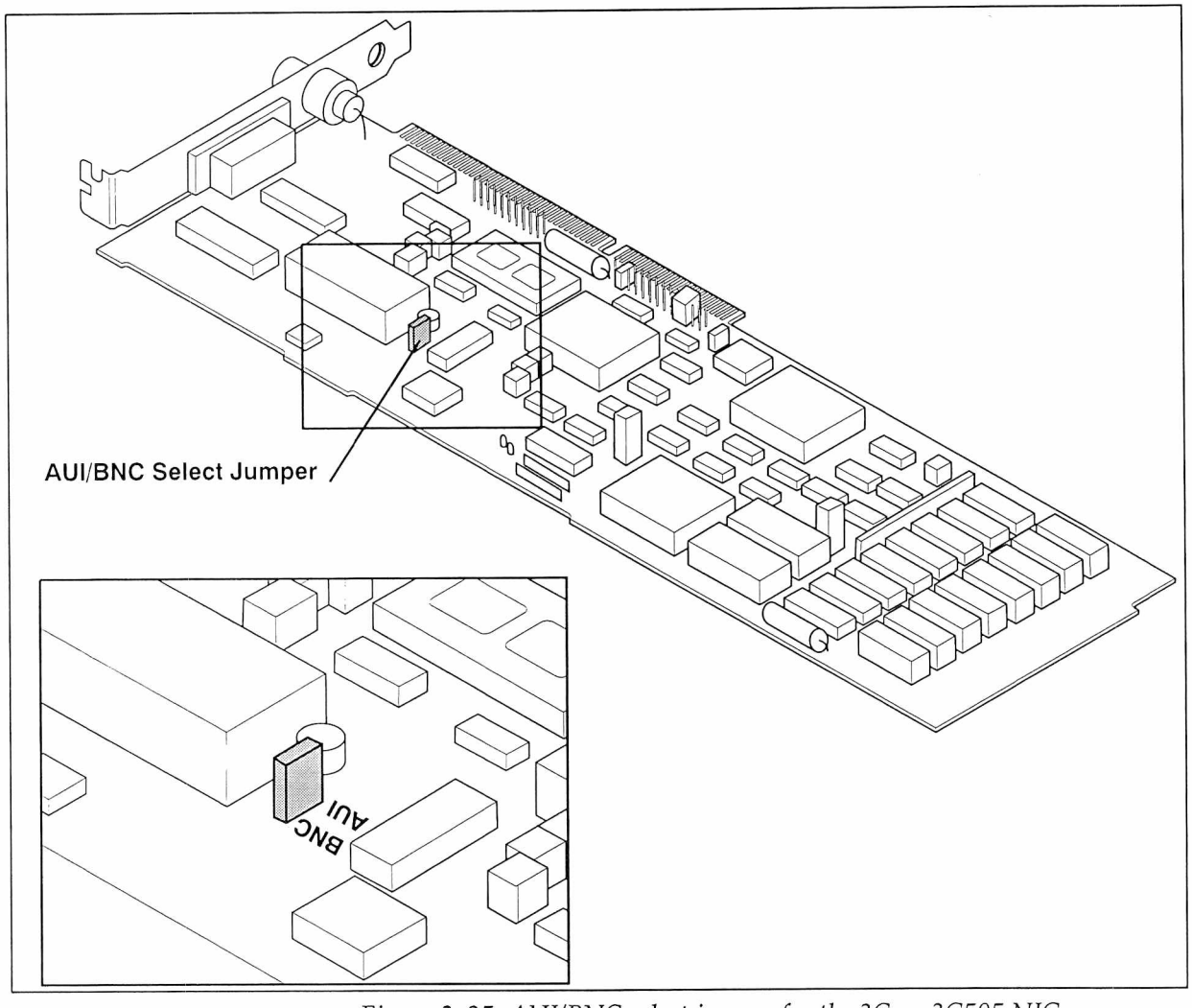


Figure 3–25. AUI/BNC select jumper for the 3Com 3C505 NIC.

Connecting Network Interface Cards

This section contains illustrations of the different types of network connectors on servers and consoles and special instructions for connecting the Ethernet and WAN cards.

Console and Server Network Connectors

Figure 3–26 shows a 16/4 token ring card with a DB-9 female connector. The token ring card works with token ring media filters as well.

You can order a token ring connector cable for the Sniffer server. This 8-ft. cable has an IBM data connector for a token ring *multiple access unit* (MAU) at one end and a male DB-9 connector at the other. You connect it by plugging the male DB-9 cable connector into the female DB-9 connector on the card. Then plug the other end of the cable into an IBM MAU model 8228 or equivalent. Always use a port numbered 1 to 8 rather than ports labeled RI or RO.

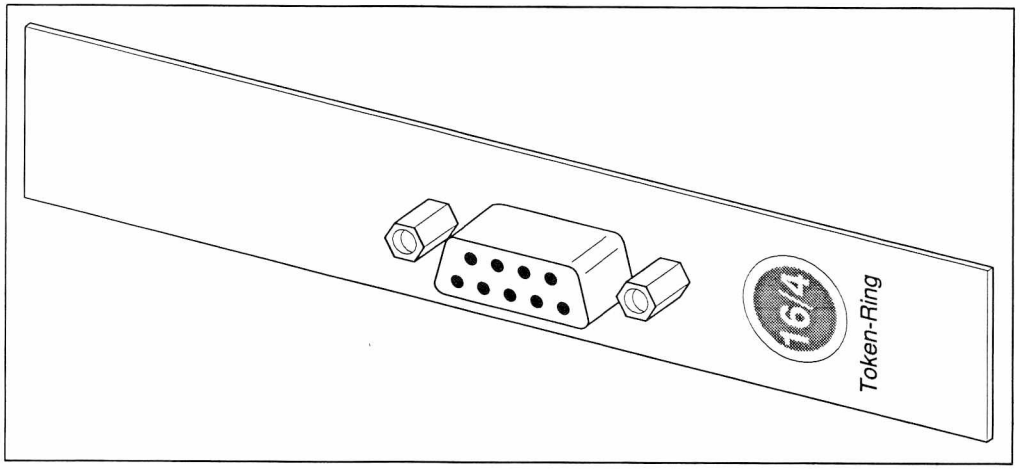


Figure 3–26. Token ring network connector.

Figure 3–27 shows two connectors on the 3Com 3C505 Ethernet card: a DB-15 connector used to attach to an external transceiver for "Thick Ethernet" and a BNC connector for "Thin Ethernet."

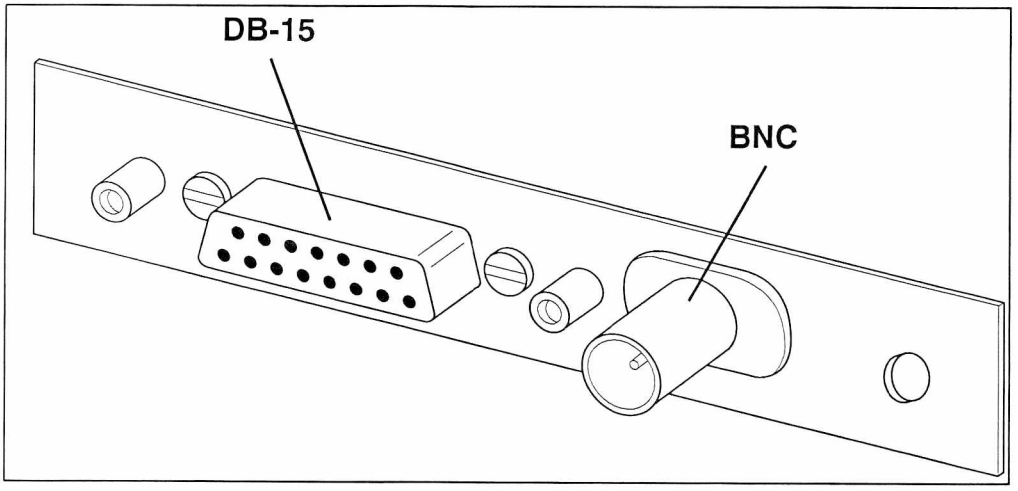


Figure 3–27. Two connectors on the 3Com 3C505 Ethernet NIC.

Figure 3–28 shows the WAN NIC with its DB-25 connector.

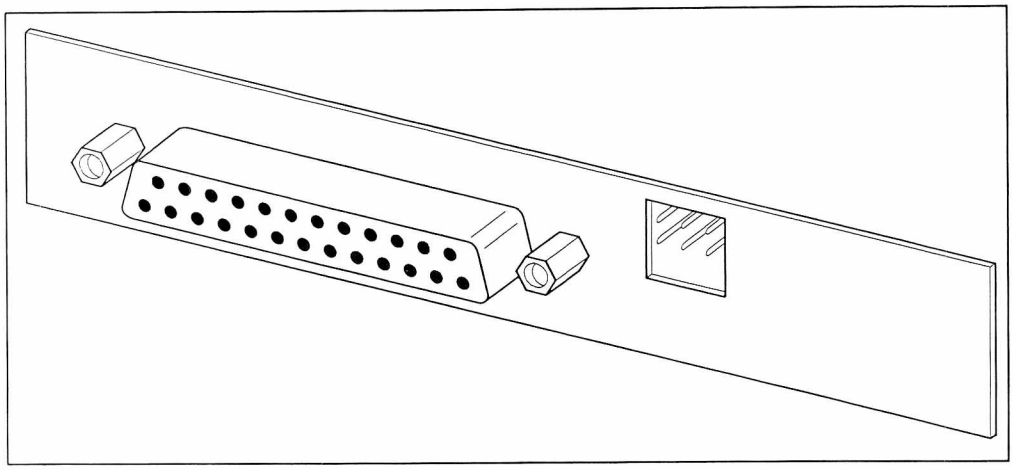


Figure 3–28. WAN DB-25 network connector.

Securing an Ethernet DB-15 Connector to the Unit

An Ethernet DB-15 cable connector is commonly secured by a slide on the cable connector that attaches to a lockpost on the device. Personal computers generally come with screw posts that secure cables by screwing them down. If you have a cable designed for lockposts, you need an adapter plate (included with the unit) to secure it to the unit's adapter card.

Install the adapter plate on the end of the cable that will be secured to the unit's Ethernet adapter card. The adapter plate clips onto the DB-15 connector. Use the screws that come with the adapter plate to secure it to the connector. If you don't need the adapter plate now, set it aside for some future occasion, and skip the following procedure.

You must use standard Ethernet transceiver cables with lockposts in order for the slide latch adapter to work with the InterLan NI5210 NIC.

To install the adapter plate for screw connections:

1. To install the adapter plate, you'll need a small flat-bladed screwdriver.
2. Slide the threaded clips onto both ends of the adapter plate (a) and insert the screws into the clips (b). At the top of Figure 3–29, you can see one of the clips positioned to slide on. At the opposite side, a clip is in place with the screw inserted.

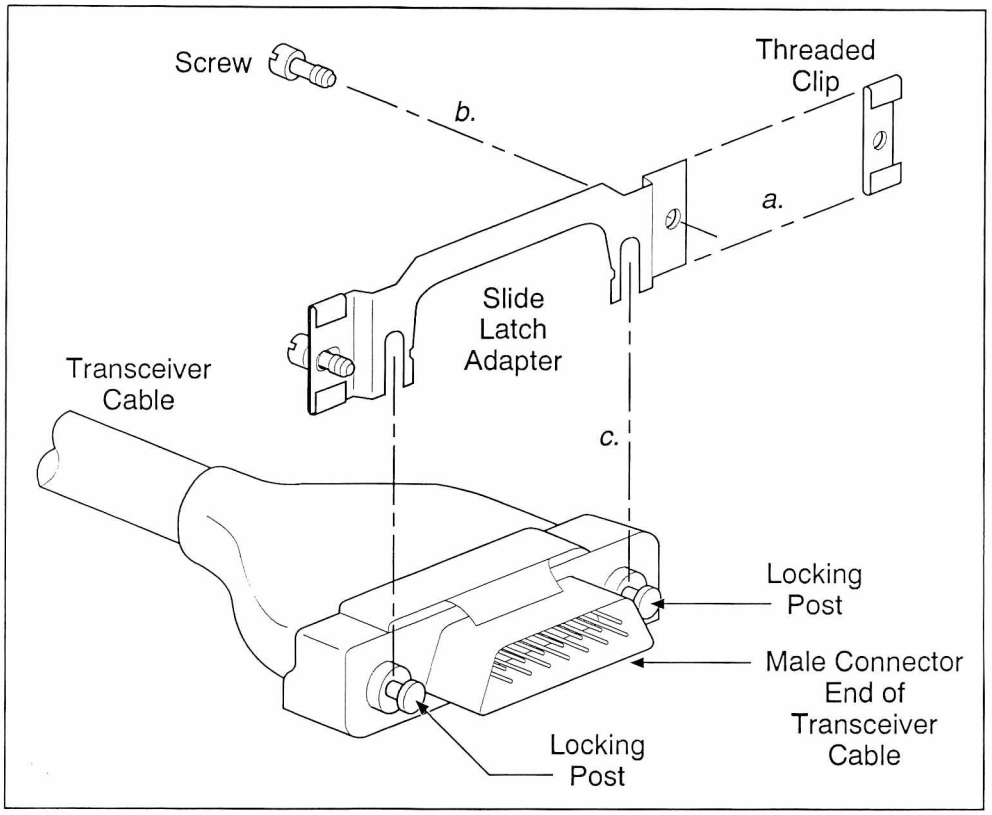


Figure 3–29. Adapter plate ready for attachment to a D-connector with lockpost.

3. Align the slots in the adapter plate with the indents in the lockposts on the transceiver cable (c).
4. Press the adapter plate until it snaps into position on the connector.
5. Plug the connector with its adapter plate into the DB-15 connector in the expansion slot.
6. Fasten the screws to the threaded receptacles above and below the connector, as shown in Figure 3–30.

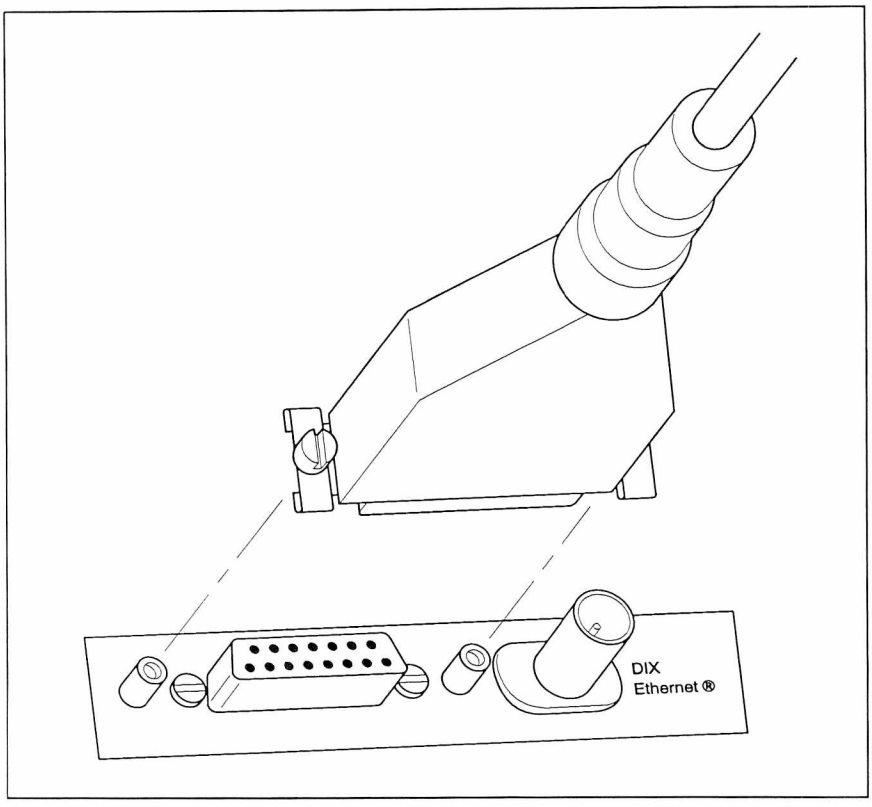


Figure 3–30. Connecting a cable with adapter plate to the unit's Ethernet card.

WAN Server

The WAN card has a DB-25 female connector (Figure 3–28) and comes with a DB-25 cable (Figure 3–31). A V.35 interface pod and cable is also included.

DB-25 Cable

The DB-25 cable accompanying each unit has three labeled connectors illustrated in Figure 3–31. Using these three connectors, you can connect your unit between either two other computers or between a computer and a modem.

To connect the DB-25 cable:

1. Attach the male-connector labeled DCE (Data Communications Equipment) to either a modem or another computer.
2. Attach the female-connector labeled DTE (Data Terminal Equipment) to another computer.
3. Attach the male-connector labeled Sniffer server to the DB-25 network connector on the Sniffer server.

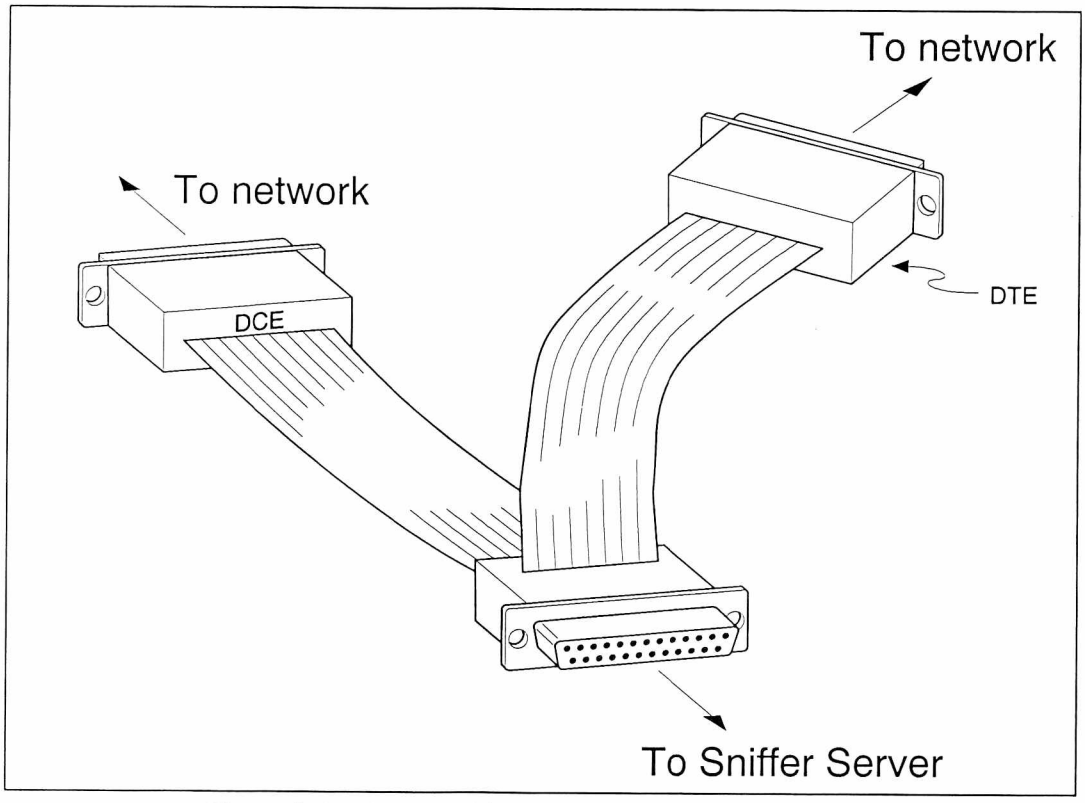


Figure 3–31. DB-25 cable with three connectors for WAN units.

V.35 Interface Pod and Cable

One option includes a V.35 interface pod and cable that converts RS-232 signals into V.35 signals (Figure 3–32).

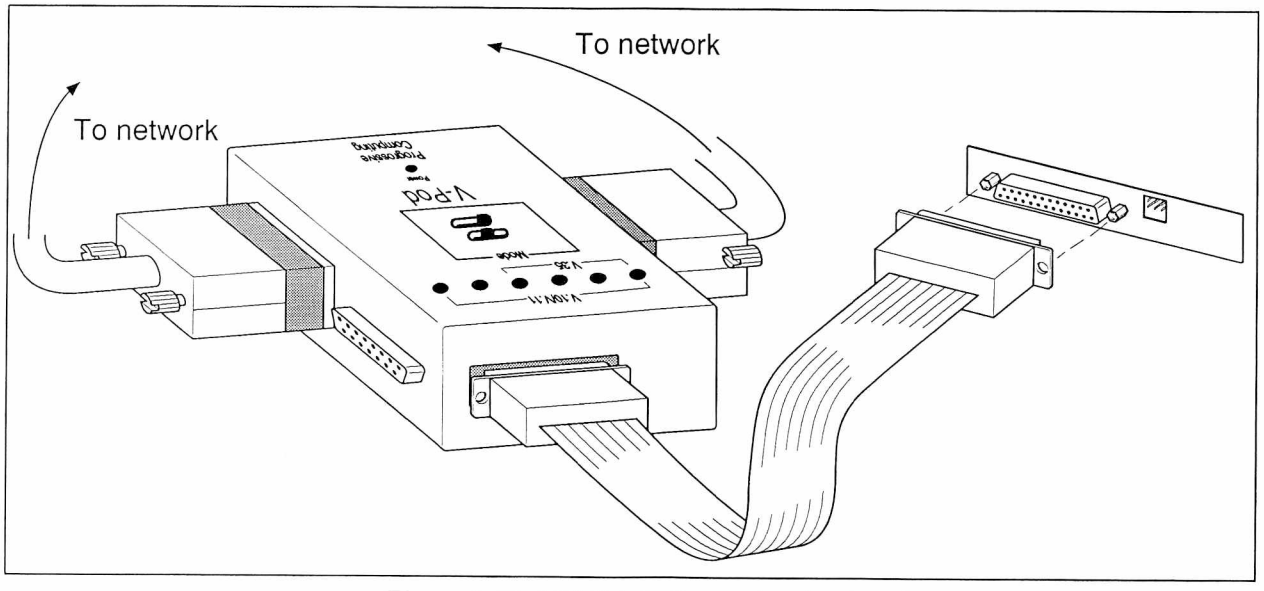


Figure 3–32. WAN interface pod and network connector.

To attach a server to a WAN network with the V.35 cable and interface pod:

1. To attach the server to a V.35 connector, you must first dismantle the existing V.35 network connection. Breaking the connection leaves one free female connector and one free male connector.
2. Network General supplies an interface pod with two female connectors on it and a V.35 cable with two male connectors. Plug one male end from the V.35 cable into the female connector from the connection you dismantled.
3. Plug the other male connector from the V.35 cable into the V.35 connector on the interface pod.
4. Plug the male connector from the connection you dismantled into the remaining female connector on the V.35 interface pod.
5. There is also a DB-25 connector at one end of the V.35 interface pod. Plug one end of the DB-25 cable into the DB-25 connection on the V.35 interface pod.
6. Plug the other end into the DB-25 connector on the server.
7. There are two female V.10/V.11 connectors on either side of the interface pod that you will not use.

CHAPTER FOUR: OPERATION OF THE DISTRIBUTED SNIFFER SYSTEM 4

Network General

Chapter 4. Operation of the Distributed Sniffer System

Chapter Overview

This chapter covers all of the functions and procedures necessary to run the Distributed Sniffer System for maximum effectiveness and efficiency. It describes how to use the console menus and keyboard to control the console and servers in the Distributed Sniffer System. The chapter also includes information on the establishment and maintenance of connections between servers and the console.

In addition, there are various ways the console provides you with system information. This chapter explains the different types of SniffMaster display and ways of formatting the displays. It also covers the auditory information used to signal you when servers connect and disconnect and when alarms are received by the console from servers. You can also select destinations for print data from the servers to console ports and files.

Operating the SniffMaster Console

A SniffMaster console allows multiple Sniffer servers to be controlled from one location. A Sniffer server is a computer providing monitoring or analysis services with which you communicate remotely from a SniffMaster console. Once the SniffMaster console has established a connection to a Sniffer server, you are "logged on" (or "connected") to it. Up to two SniffMaster consoles may be logged on to a single server at a time. When you are not logged on to a Sniffer server, you are "disconnected."

At times you will be looking at the menus and screens of the console that allow you to manage and to select Sniffer servers. Other times you will be looking at a Sniffer server screen. When you can see a server screen on the console's display, you can then control it from the console's keyboard.

The user interfaces of both the console and the servers are similar, so you don't have to learn a new style. They are so similar, in fact, that you may occasionally wonder what you are looking at. But as described later, the F12 (**Menus**) key will always get you to the Main Menu of the console.

Modes of Operation

Menu-driven Controls

Menus control all the SniffMaster console's functions. Move the cursor to the option you want, and press Enter or Spacebar to register your choice. Or, press one of the function keys. Function keys are always labeled on screen to show their operation. Most actions require only that you move the cursor, and press a key. A few actions cause the SniffMaster console to open a dialog box in which you supply details (for example, a name or address).

Menu Tree

When you start the SniffMaster console, the screen displays the Main Menu. Figure 4–1 shows an example of the Main Menu in the center panel with the Control Servers menu in the right panel

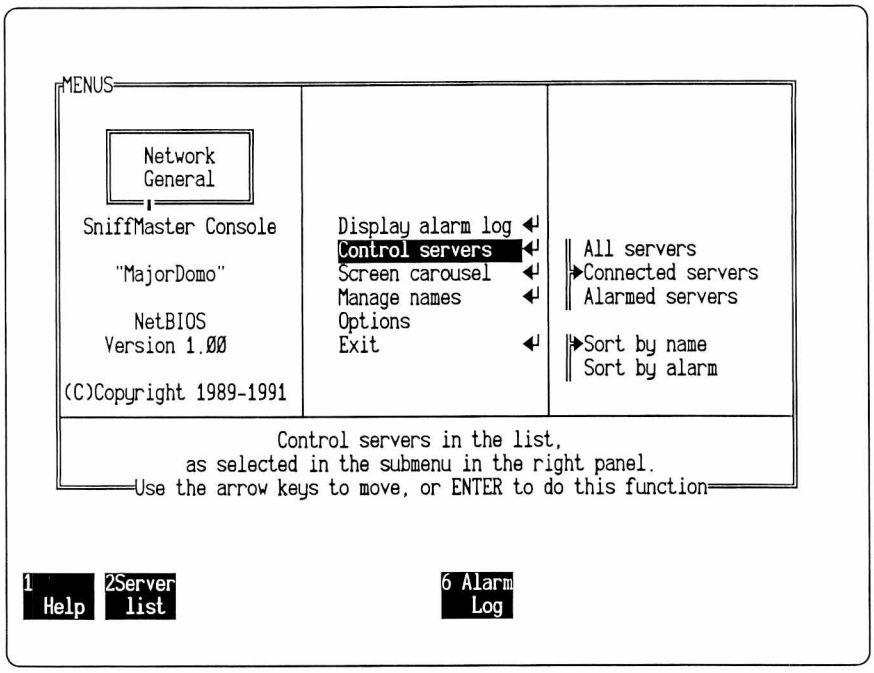


Figure 4–1. SniffMaster console's Main Menu in the center panel and Control Servers menu in the right panel.

The entire menu structure is a tree, with its root (the Main Menu) to the left and its branches and leaves (menus of options in a given menu) to the right. Figure 4–2 shows the menu structure of the SniffMaster console.

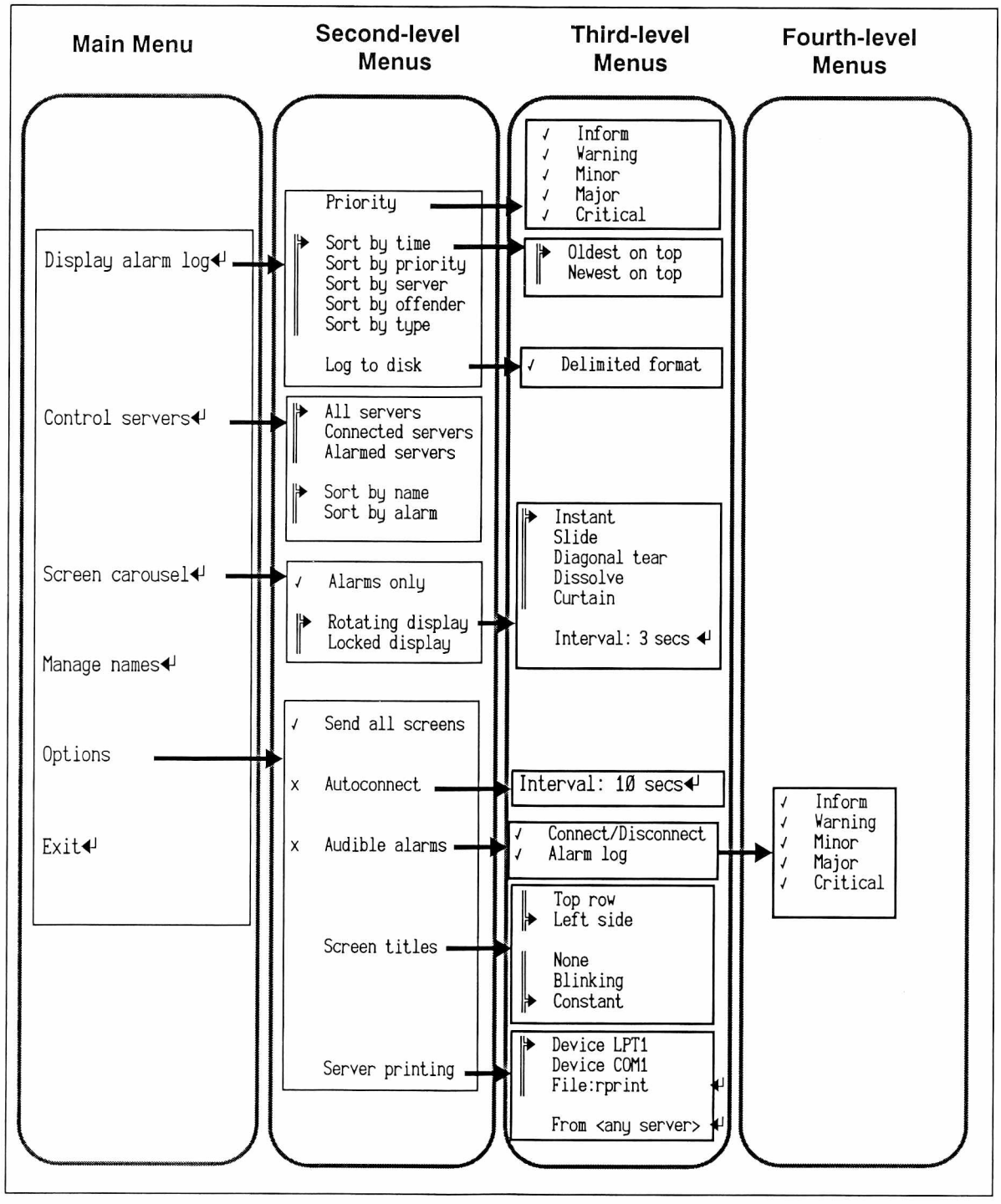


Figure 4–2. SniffMaster console menu tree.

When the SniffMaster console starts up, the screen shows three panels side-by-side. You control the center panel. Within that center panel, the center row is highlighted. That is your location in the menu. When you first start the SniffMaster console, the center panel lists the

alternatives available from the root of the tree. Some alternatives appear above the highlight, some below it. Initially, the highlight is on **Control servers**.

When you press the Cursor Up key, the item above **Control servers** becomes highlighted. We speak of "moving the highlight up" to the next item. The highlight doesn't really move; instead, the entire center panel scrolls downward so that the (stationary) highlight is now on the row above.

The panel to the right shows choices in the menu that go with the item highlighted in the center panel. As soon as you bring a different item to the center highlight, the entire right panel changes. The right panel always shows the menu that goes with the item that's highlighted in the center (see Figure 4–2).

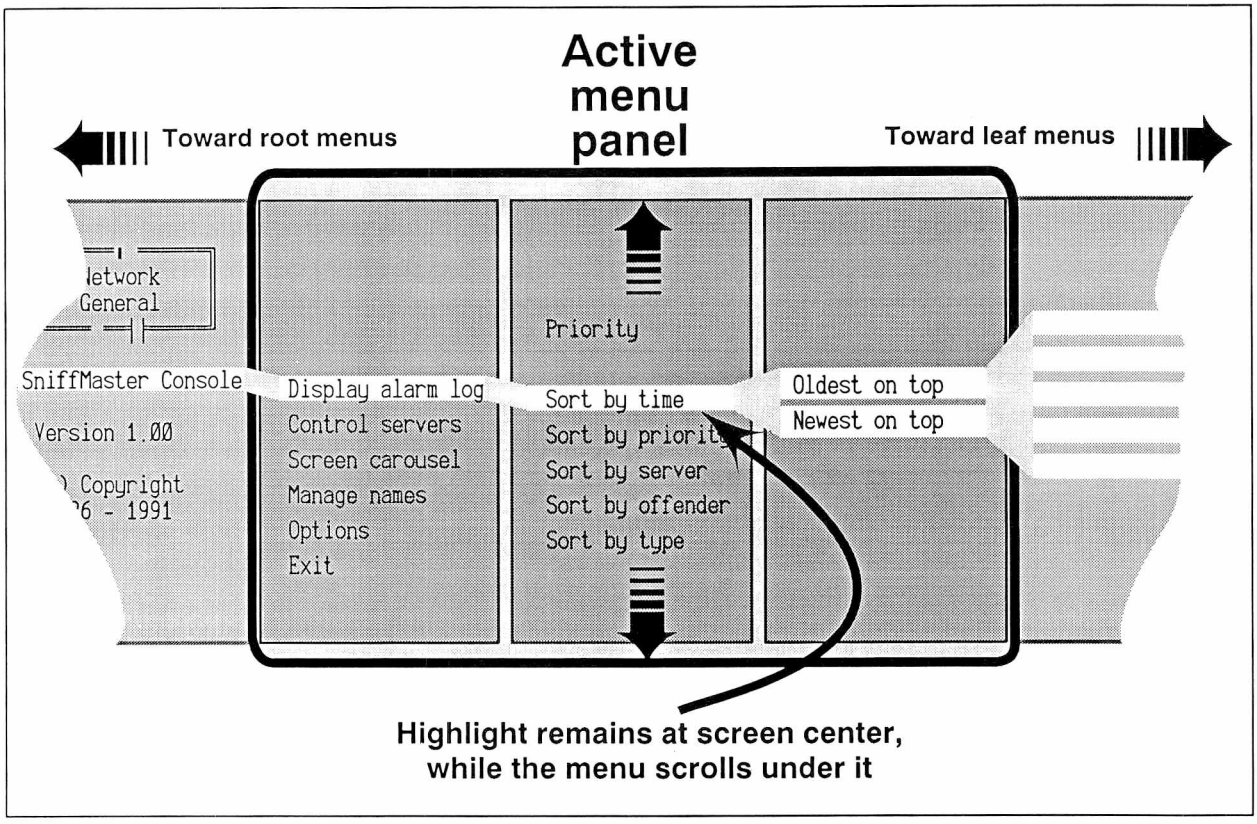


Figure 4–3. Diagram to illustrate scrolling over the tree-structured menu.

To select one of the options in the right panel, press the Cursor Right key. It's as if you move rightward from the center of the screen. The highlight doesn't really move. Instead, the entire menu structure moves leftward under the highlight panel. The panel that was to the right now moves to the center. The panel that was in the center now moves to the left. The panel that was at the left vanishes, as though it moved out of sight beyond the left edge of the screen.

If the new center item has options associated with it, they appear in the right panel. Sub-menus seem to move in from beyond the screen's right edge. When the item in the center has no options, the right panel is blank.

The four Cursor keys permit you to traverse the entire menu tree. Your current selection always appears at the center of the center panel, with other choices at the same level above and below it. The right panel shows the sub-menus (if there are any), and the left panel shows the menu nearer the root (or the Network General logo when you're at the root).

If you have problems with the Cursor keys, check that the NumLock key has not been accidently depressed. If the NumLock indicator light is "on," press the NumLock key once more to reset the keypad to normal function so that the Cursor keys are active.

Shortcuts

There are two shortcuts you will find very useful:

- You can move to the first item in a vertical list by pressing the Home key and to the last item by pressing the End key.
- You may press the first letter of the item name to jump to that item. If two or more items have the same first letter, repeated depressions of that letter key will select items sequentially from top to bottom.

Menu Conventions

The menus contain two kinds of items: actions and options. First you set options; then you start an action involving them.

Options

An option specifies how an action will work when it starts at some future time. Examples of options are:

- Choosing between a rotating carousel display and a locked carousel display.
- Selecting which alarm priority levels will show in the Alarm Log.
- Determining whether or not to have the console try to connect automatically to all servers in its data base at an interval you choose.

There are two kinds of options. A *checklist* is a list of items. Put a ✓ beside each item that you want, an x beside those you don't want. You can check as many or as few as needed. A *radio control* is a list of mutually exclusive options (so called because, like a push-button

radio, selecting one deselects the others). A radio control has a vertical bar beside it, and an arrowhead at the selected item, thus:

```
▶ Selected item
  Deselected item
```

To change an option:

1. Position the highlight on the option you want.
2. Press Spacebar.
   - On a *radio control*, pressing Spacebar moves the arrowhead to the highlighted item.
   - On a *checklist*, pressing Spacebar changes ✓ to x (or x to ✓).
3. Holding down the Alt key while pressing Spacebar reverses the setting of all items in the list.

Actions

When you press the key for an action, something starts to happen. Some examples of actions are:

- Press the function key, F6, to display the Alarm Log. When you are connected to one or more servers, you will see alarms. Consoles accept alarms from servers at the priority level selected using the Display Alarm Log\Priority menu.
- Press the Enter key when the highlight is on the Manage names item of the Main Menu. This opens the console's data base so you can add servers to the data base, delete servers, or change name and address information about the servers.

To start an action:

1. Position the highlight on the action you want.
2. Press Enter.

   An action that can be started by pressing Enter always has ↵ beside it.
3. Alternatively, press the appropriate function key.

Function Key Menus

Function keys provide a quick way to begin certain frequently performed activities that are also available from the menus. For example, you may display the alarm log by pressing F6, or you may select **Alarm log** via the menus. They are equivalent, and the choice is yours.

A function key identifier will appear at the bottom of the screen only if starting that activity is reasonable at the moment. (This is not true for the menu entries they represent, which are always present so that you can see all possibilities.) For example, F9 (**Screen carousel**) is seen only when at least one Sniffer server is connected and available for display.

The significance of some of the function keys changes depending on the current context. For example, when you are in the Server List display, the F7 key will "connect" if the Sniffer server you are highlighting is not connected, and "disconnect" if the Sniffer server is already connected.

Notice the three function keys labeled at the bottom of the Main Menu shown in Figure 4–1: F1 (**Help**), F2 (**Server list**), and F6 (**Alarm log**). This is a menu of currently active function keys. If you were to press F2, for example, a window would open showing you a list of Sniffer servers currently registered with this SniffMaster console. The items on the function key menu vary according to where you are in the menu tree.

The table in Figure 4–4 lists the functions keys available at various states of the SniffMaster console.

Function Key	Menus	Server Status	Alarm Log	Special Windows	Screen Carousel
F1	Help	Help	Help	Help	
F2	Server list		Server list		
F3		Misc. control	Ack alarm		
F4			Clear alarm		
F5		Menus	Menus		
F6	Alarm log	Alarm log			
F7		Connect/ Disconnect			
F8		Server screen	Server screen		
F9	Screen carousel	Screen carousel	Screen carousel		
F10					
F11					Next/ List
Shift-F11					Previous
F12					Menus

Figure 4–4. Functions keys available at various states of the SniffMaster console.

Using On-Line Help

The console provides an on-line help facility that displays information about the following topics:

- Moving around in the menus
- Selecting a menu item
- Using the function keys
- Managing the list of servers
- The Server Status display

- Configuring the Server Status display
- Using the Server Status display
- The Alarm Log
- Using the Alarm Log
- Saving alarm information to a file
- The screen carousel
- Operating the screen carousel
- Configuring the screen carousel display
- Automatic connections
- Controlling sounds
- Controlling server print output
- Updating console and server software
- Transferring files
- Rebooting a server
- SNMP Network Management Stations

To use on-line help:

1. Press F1 (**Help**).

   Result: A window opens displaying the Help Index.

2. Use the Cursor Up or the Cursor Down keys to highlight the topic of your choice.

3. Press Enter.

   Result: A second window opens over the first and displays detailed information about the topic.

4. Use the Page Up and Page Down keys to scroll to additional information on the topic.

5. Press the Esc key to return to the Help Index.

6. Press the Esc key again to return to the screen displayed before you used on-line help.

Displays and the Use of Color

If you are using a color screen, the SniffMaster console uses light-colored menus and the Sniffer servers use dark-colored menus, which helps distinguish between the two.

The default for the SniffMaster console is color. If you have some other type of display, you can select screen attributes for the console that will enhance it. You can choose monochrome, plasma, liquid crystal display, or gray-scale:

To select console screen attributes:

1. Exit the console application to DOS.
2. At the DOS prompt, type

   C:\CD CONSOLE
3. Press the Enter key.
4. Open the first batch file used to start the SniffMaster console software using the DOS line editor, EDLIN, or some other text editor. This could be in CONSOLE.BAT supplied by Network General or a special startup batch file you created.
5. Find the two lines in the file containing the command to execute both versions of the SniffMaster software. The command is TCONSOLE for a TCP/IP console and NCONSOLE for a NetBIOS console.
6. Add the appropriate command-line parameter for the screen attribute you want:
   - MONO monochrome
   - PLASMA plasma
   - LCD liquid crystal display
   - GRAY gray-scale

   For example, enter TCONSOLE MONO to start the TCP/IP SniffMaster software in monochrome, instead of color.

   Remember that the screen attribute you choose for the console must match that of your servers. For instructions on changing the server configuration, see "To configure a Sniffer server:" on page 3–14.
7. Save the batch file.
8. Open the second batch used to start up the console, NGCEXEC.BAT using the DOS line editor, EDLIN, or some other text editor.
9. Find the line containing the command to invoke the console.
10. Repeat Steps 6 and 7.

Connections Between the Console and its Servers

This section describes how to set up, to establish, and to maintain basic connections between SniffMaster consoles and Sniffer servers. There are three basic areas of relationship:

- Managing the names of Sniffer servers
- Controlling Sniffer servers from the SniffMaster console
- Other types of controls

Before any communication can take place between a console and servers, you need to record the names of the servers at the console. The console has a special display that you'll use to control the servers. You have various options for configuring that display, for establishing connections with the servers, and for displaying server screens on the console. Finally, other controls of servers are available, including uploading and downloading files and rebooting servers from the console.

Managing Names

The **Manage names** item on the main menu (Figure 4–5) allows you to add to, remove, or change the Sniffer servers that are known to the SniffMaster console. Once you include the relevant server information in the console's data base, you can connect to servers either manually or automatically.

When you add servers to the console's data base, you enter both a symbolic name and a NetBIOS or TCP/IP transport address. The symbolic name will be used in displays like the Server Status display and the Alarm Log display. The symbolic name also shows up in the screen title that appears in the top row or the extreme left column whenever you are looking at server screens. There is a 31-character maximum for symbolic names.

The NetBIOS transport address you enter is the one that came with your server, and you must derive it from the Transport Card address to be found on the label attached to the bottom of the server. Instructions for deriving it are in "To derive the NetBIOS address for each Sniffer server:" on page 3–36. However, if you substituted an address for the NetBIOS address assigned by NGC when you configured the server, be sure to enter that one. NetBIOS addresses are case-sensitive.

The console and server symbolic names and server NetBIOS or TCP/IP transport addresses you enter here are stored in the STARTUP.SNM file located in the same directory as the console software. The file also contains the name you assigned the console when you first started it up. You will want to back that file up periodically.

A NetBIOS file has the following format:

```
ourname "MajorDomo"
server name "TP Analyzer" addr NetBIOS "rumplestiltskin"
server name "TP Monitor" addr NetBIOS "NGCTB7789d"
```

A TCP/IP file has a similar format:

```
ourname "MajorDomo"
server name "BIZ-ONE Server" addr TCP/IP "16.Ø.1Ø5.21"
```

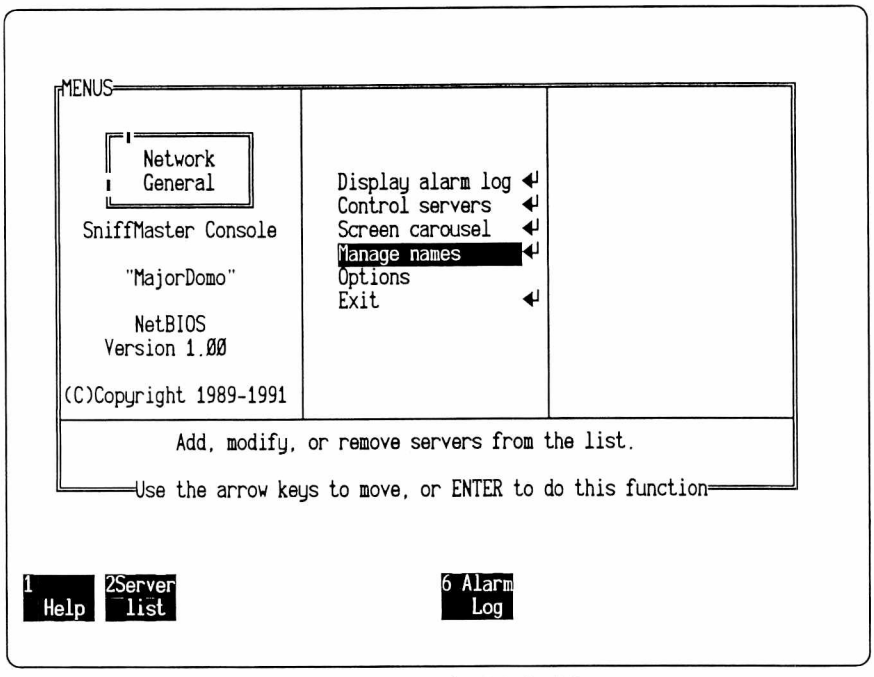


Figure 4–5. **Manage names** *item on the Main Menu.*

To add a new Sniffer server to the Manage Names list:

1. Use the Cursor keys to highlight the **Manage names** item on the Main Menu.
2. Press Enter to open the **Manage Names** list (Figure 4–6).

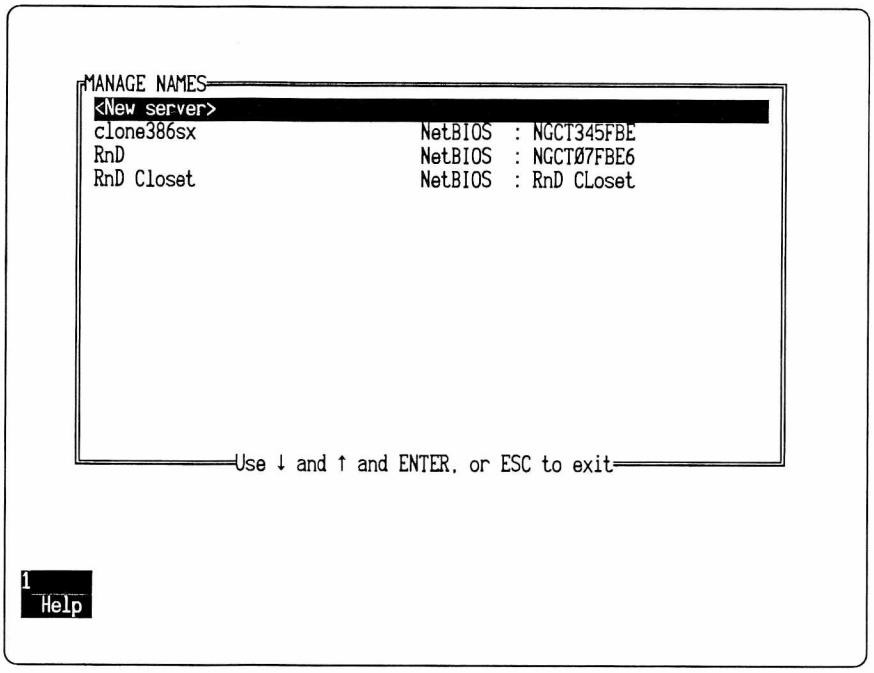


Figure 4–6. Manage Names list.

3. With the highlight on **<New server>**, press Enter.

   Result: A window appears for entering a symbolic name for the Sniffer server (Figure 4–7).

4. Type the symbolic name to use for the Sniffer server.

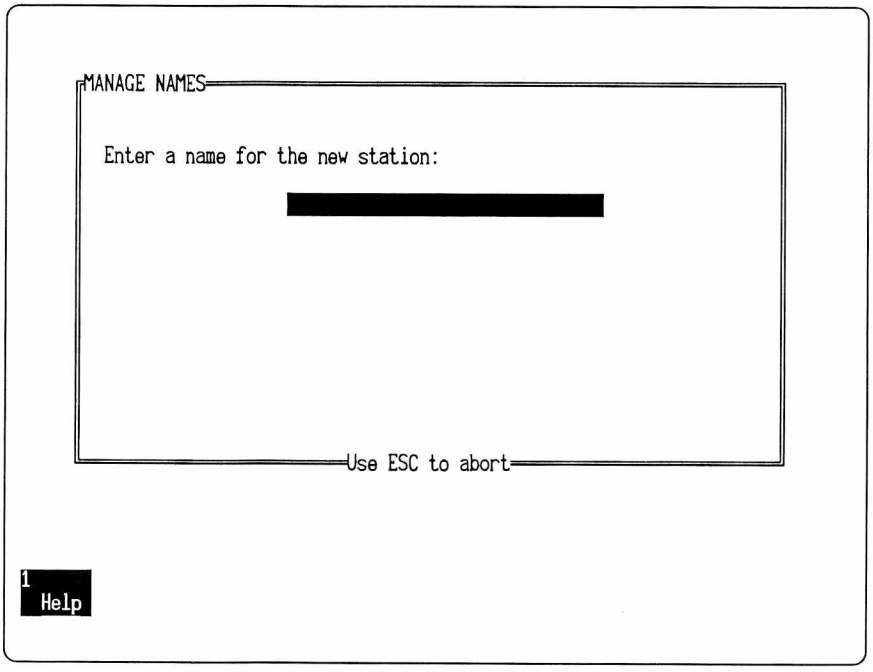


Figure 4–7. Manage Names dialog box for entering station name.

5. Press Enter.

   Result: A window for entering a transport address appears on the screen (Figure 4–8 for NetBIOS and Figure 4–9 for TCP/IP).

6. Type the address in the field provided. The format you use depends on the transport protocol. Are you entering a NetBIOS address or a TCP/IP address?

   - If it's a NetBIOS address, you can use up to 16 characters. The address is space and case sensitive. You must use the address you entered when you configured the server. See Figure 4–8.

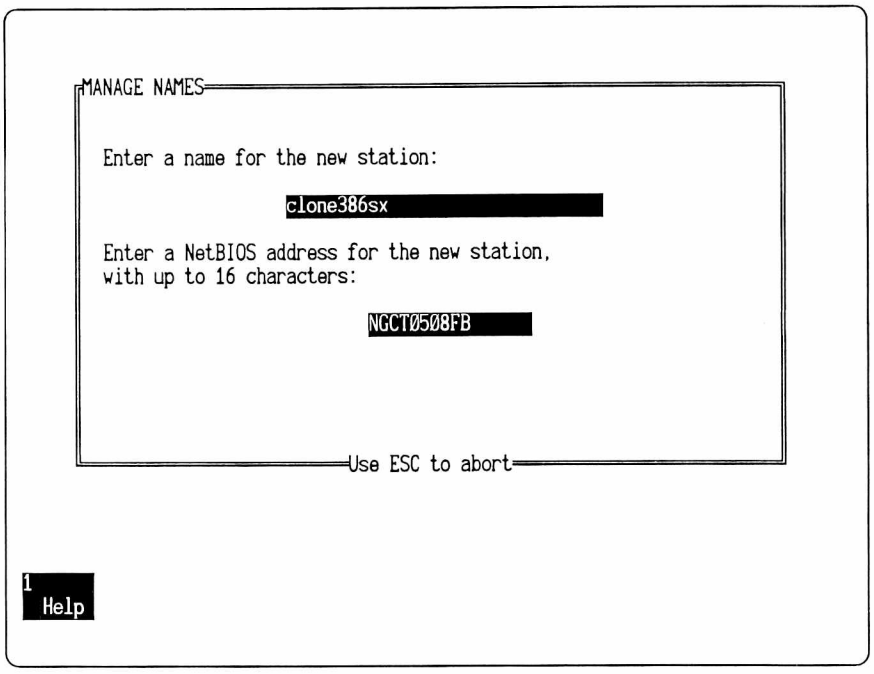


Figure 4–8. Dialog box for entering a new NetBIOS address.

   - If it's a TCP/IP address, use dotted decimal notation. You must use the address you entered when you configured the server. See Figure 4–9.

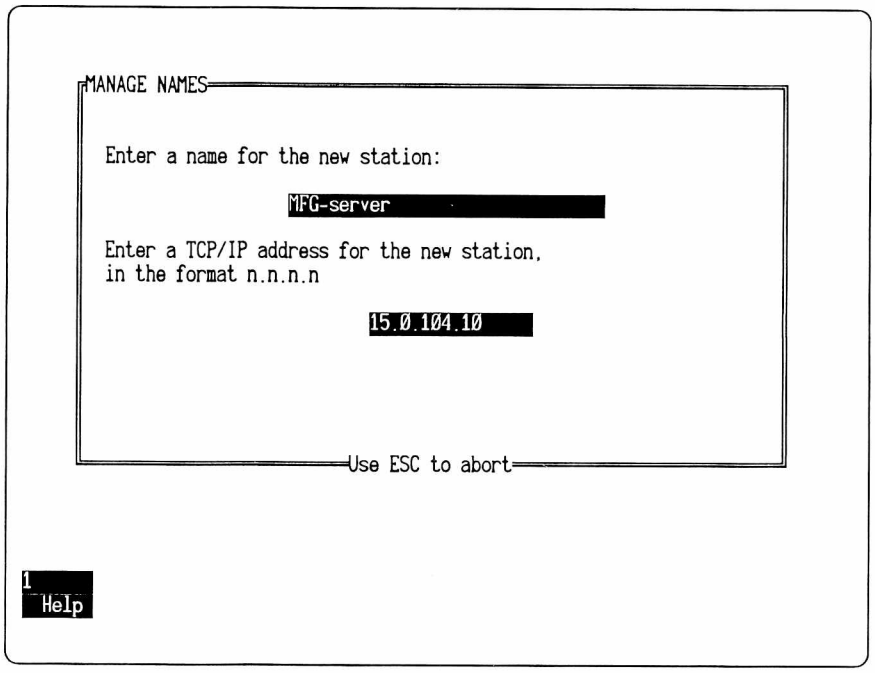


Figure 4–9. Dialog box for entering a new TCP/IP address.

7. Press Enter.

To remove a Sniffer server from the Manage Names list:

1. Use the Cursor keys to highlight that Sniffer server's name in the **Manage Names** list (Figure 4–6).
2. Press Enter.

   Result: A message appears on the screen:

   ```
   Press DEL to delete this server
   ```

3. Press the Delete key.

   Result: A warning window pops up to confirm the operations, and then the Sniffer server's name will be removed from the table.

To change the name or transport address of a Sniffer server:

1. Use the highlight to move the highlight that Sniffer server's name in the **Manage Names** list (Figure 4–6).
2. Press Enter.

   Result: The Manage Names dialog box appears on the screen (Figure 4–7).

3. See the procedure, "To add a new Sniffer server to the Manage Names list:" on page 4–14. You will be prompted to change the name and the transport address in turn.

   Note: Sniffer servers may be changed or deleted only if you are not currently connected to them.

Controlling Sniffer Servers

Once you have the names and addresses of Sniffer servers in the SniffMaster console's list of Sniffer servers, you are ready to establish connections with the Sniffer servers, to display their screens, and to control their operation through the facilities of the SniffMaster console.

You access these capabilities through the Server Status display. See the section, "Using the Server Status Display to Control Servers" on page 4–20. You can also format the Server Status display to make it more readable and useful for your particular purposes. See the next section, "Formatting the Server Status Display."

Formatting the Server Status Display

The Server Status display provides information on some or all of the Sniffer servers in the SniffMaster console's data base. The display also provides the major controls for Sniffer servers. Figure 4–12 shows an example of a Server Status display.

On the Control Servers menu, there are two option lists with choices for what will appear on a Server Status display (Figure 4–10).

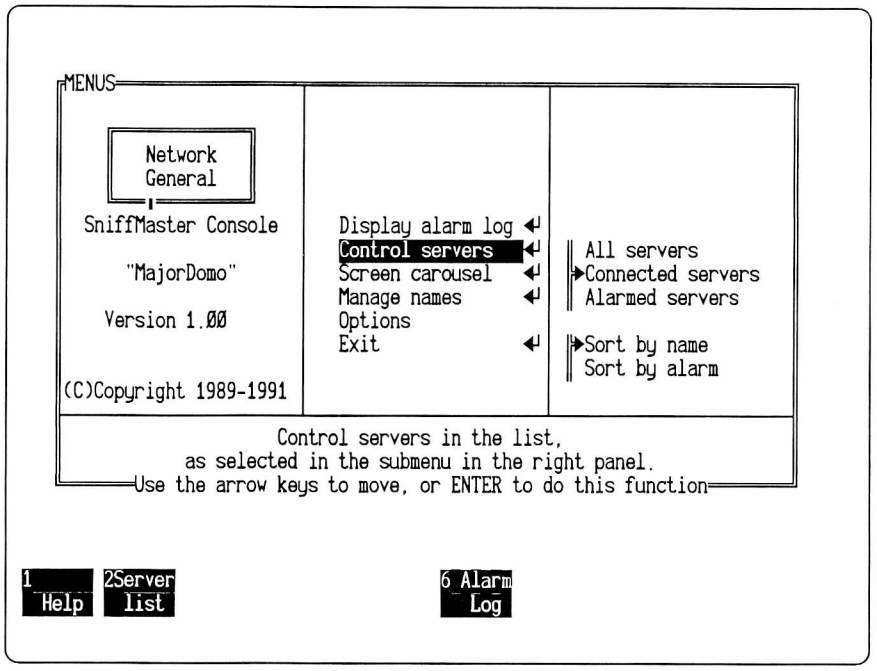


Figure 4–10. Control Servers menu.

One option list lets you determine which Sniffer servers will be listed in the Server Status display. The second option list allows you to decide the order in which the Sniffer servers will be listed. The table in Figure 4–11 shows the options in each list:

Option List	Option	Function
Sniffer servers to show	All servers	Lists all connected and unconnected Sniffer servers.
	Connected servers	Lists only connected servers.
	Alarmed servers	Lists only servers in "alarmed" state.
Sort criteria	Sort by name	Lists in alphabetical order by server name.
	Sort by alarm	Lists by maximum alarm priority on the server.

Figure 4–11. Options for Server list display format.

To determine which Sniffer servers will be shown on the Server Status list and in what order:

1. With the highlight on **Control servers**, use the Cursor Right key to move the highlight to the Control Servers menu (Figure 4–10).

2. Use the Cursor Up and Cursor Down keys to move the highlight to one of the two checklists in the menu and then to the option you want to select.
3. Press the Spacebar.

   Result: The pointer will move to the item of your choice.
4. Repeat steps 2 and 3 for the other option list.

Using the Server Status Display to Control Servers

The Server Status display gives you control over the Sniffer servers. The Sniffer server controls available from this display are:

- Connecting and disconnecting from Sniffer servers. Besides connecting from the Server Status display, you can also enable the console to connect to servers automatically. The autoconnect function of the console will periodically try to connect to Sniffer servers which are on the list but not currently logged on to the console. This is done continuously in the background as long as Sniffer servers remain logged off. You can specify the time interval between connection attempts. A connection to one unconnected Sniffer server is attempted at the end of each interval, in round-robin fashion. The autoconnect function will skip any server that requires a password.
- Once connected to a monitor server, running the monitor application in background. This lets you continue to observe a network segment or ring while you perform other tasks on the server from the console.
- Displaying Sniffer server screens individually or in a carousel format. Before you display the carousel format, you can opt for transition effects between server screens as well as the time interval between transitions.
- Displaying the Alarm Log with alarm information from Sniffer servers. Before displaying the Alarm Log, you can format it in several ways, i.e., to filter for alarm priority levels before they are received and to sort alarms by various criteria.
- Miscellaneous controls for logged on servers, including updating Sniffer server software, uploading files to the SniffMaster console, downloading files to the Sniffer server, and rebooting the Sniffer server. These controls are explained in "Miscellaneous Control" on page 4–33.

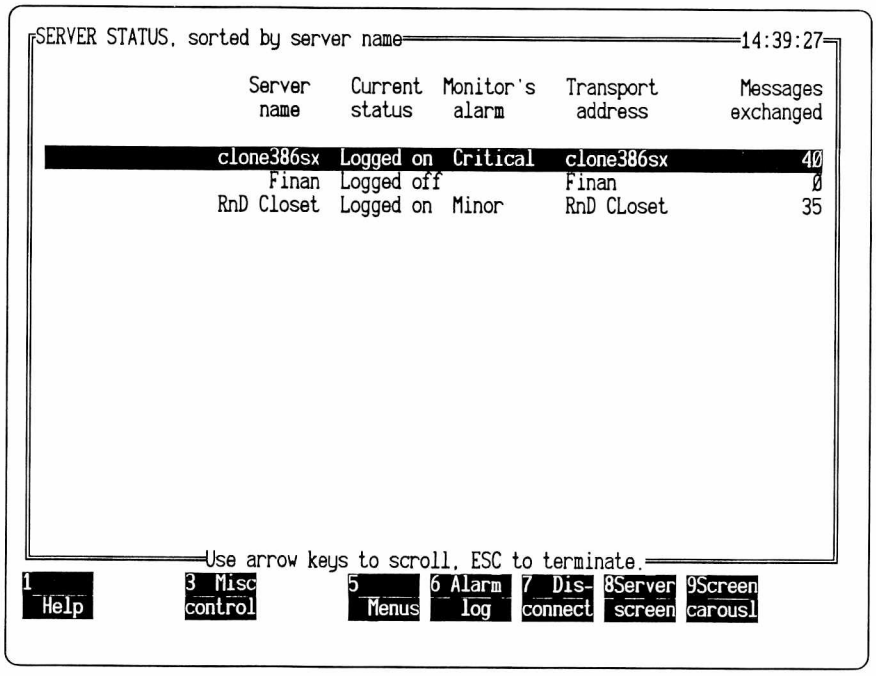


Figure 4–12. Server Status list of Sniffer servers.

To open the Server Status display:

1. Use the Cursor keys to move the highlight to **Control servers**.
2. Press Enter.
3. Alternatively, use F2 (**Server list**) if it is active.

To connect to a Sniffer server:

1. Use the Cursor Up or Cursor Down key to move the highlight to the Sniffer server to which you want to connect.
2. Press F7 (**Connect**) or, alternatively, Enter.
   - If you are connecting to a server, and the server is *not* configured with a password, the indication in the Current Status column of the Server Status display changes to "Logged on":
     a. Press F8 (**Server screen**) or, alternatively, Enter.

        Result: The server's Main Selection Menu appears.

     b. Go to the next step.
   - If you are connecting to a server, and if that server is configured with a password, a field for entering the password appears (Figure 4–13).

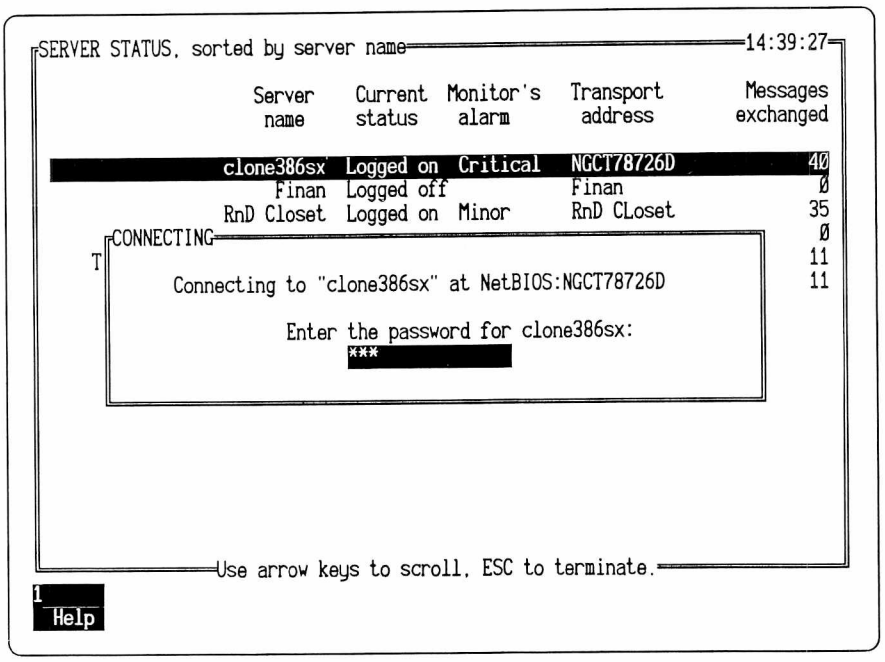


Figure 4–13. Field for entering the server's password.

a. Type the password.

b. Press Enter.

   Result: The message in the Current Status column of the display changes to indicate whether the Sniffer server is "Logged on." If you enabled the sounds options, you will also hear a musical chime.

   Note: When you enter an invalid password, a window pops up telling you that.

c. Press F8 (**Server screen**) or, alternatively, Enter.

   Result: The server's Main Selection Menu appears (Figure 4–14).

d. Go to the next step.

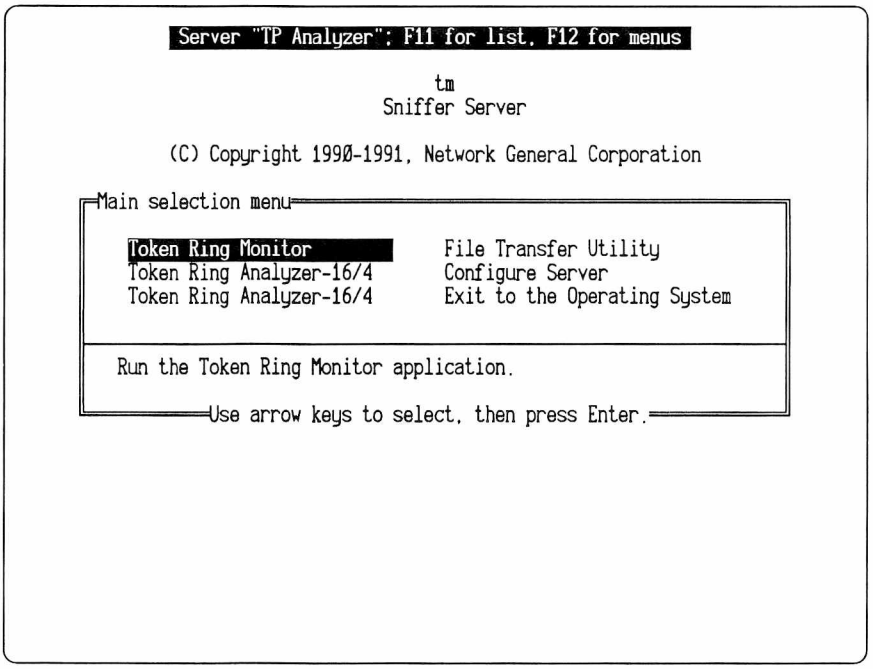


Figure 4–14. Analysis server Main Selection Menu.

- Note: If no contact is made with the server—i.e. the indication in the Current Status column reads "Logging on" then reverts to "Logged off" or the indication reads "Lost"—check Appendix A., "Troubleshooting Guide."

3. Use the Cursor key to highlight the server application you want to load at the server. Do you want an *analysis* application or a *monitor* application?

   - If you choose an *analysis* application:

     a. Press Enter.

        Result: The application is loaded, and the analyzer server initialization screen appears (Figure 4–15).

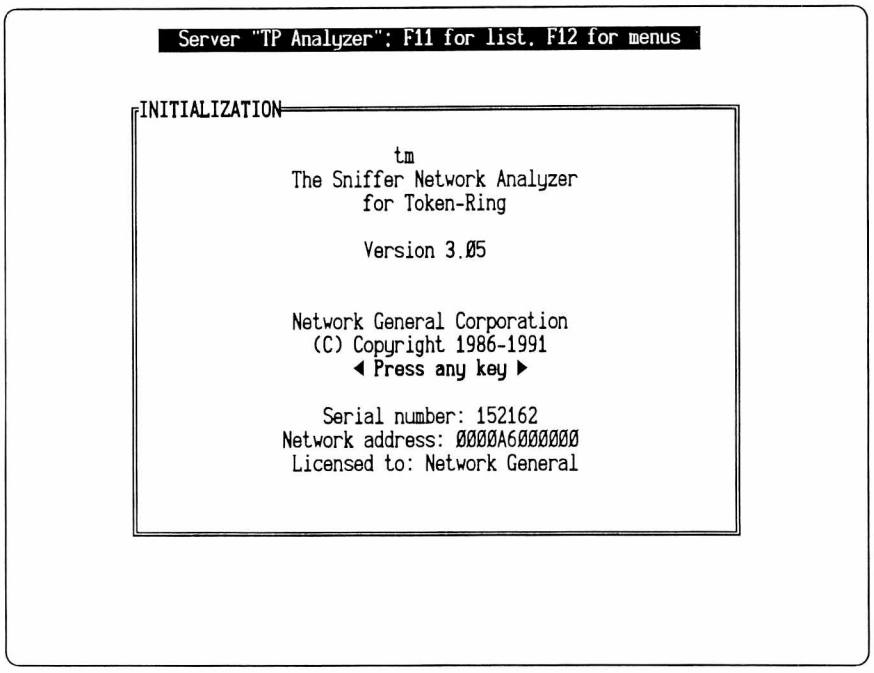


Figure 4–15. Analysis server initialization screen.

b. Press any key when prompted.

Result: The analysis server Main Menu appears (Figure 4–16).

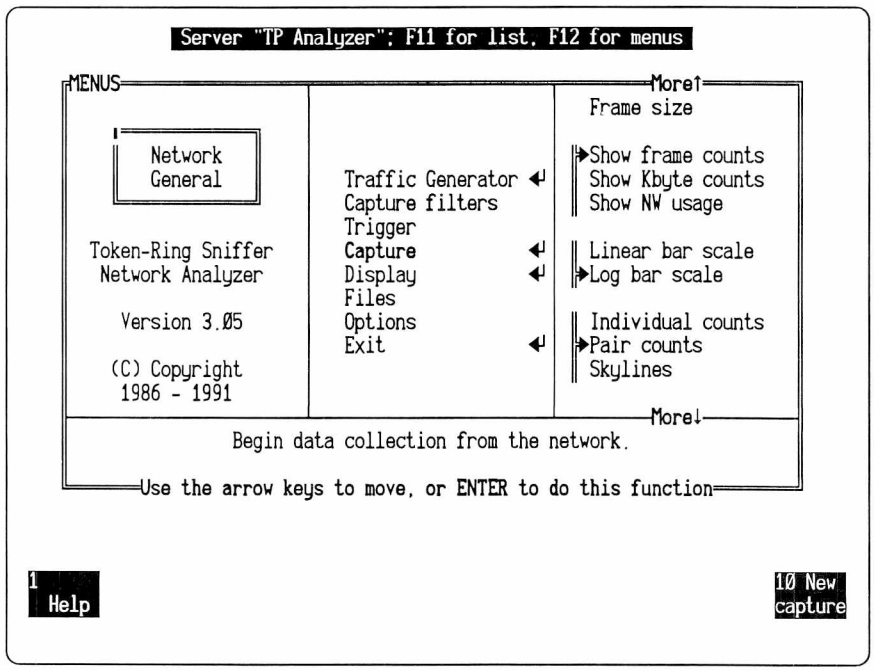


Figure 4–16. Analysis server Main Menu.

Note: You are now ready to start using the analysis

server to observe the network segment, ring, or link to which it is attached. For more information on operating the analysis server, see the *Distributed Sniffer System: Analyzer Operations Manual.*

- If you choose a *monitor* application:

  a. Press Enter.

  Result: The application is loaded, and the monitor server initialization screen appears.

  b. Press any key when prompted.

  Result: The monitor server Main Menu appears.

  Note: You are now ready to start using the monitor server to observe the network segment or ring to which it is attached. For more information on operating the monitor server, see the *Distributed Sniffer System: Token Ring Monitor Operations Manual* or the *Distributed Sniffer System: Ethernet Monitor Operations Manual.*

  Note: Monitor applications are loaded in two parts. One part runs in background—e.g., collecting statistics—and lets you use the server for other purposes. The other part is a user interface. Once you've loaded the background processes, you do not have to reload them and can invoke the user interface whenever you want to access the background processes.

  However, you cannot run an analyzer application at the same time that you are running a monitor in background. You will be prompted to shut the background processes down when you try to start the analyzer application.

  Another caveat is that, while statistics are still being collected, alarms are not sent to consoles when a monitor is running in background.

  See the procedure "To use the monitor application in the background:" on page 4–25 for further instructions.

To use the monitor application in the background:

1. Use the Cursor keys to highlight the monitor application in the server's Main Selection Menu (Figure 4–14).
2. Press Enter.

   Result: The monitor server's initialization screen appears.
3. Press any key when prompted.

   Result: The monitor server's Main Menu appears.

4. Use the Cursor to highlight **Exit** on the Main Menu.
5. Press Enter.

   Result: The user interface part of the monitor application is unloaded, the background processes part is still running, and the server's Main Selection Menu appears again. At this point you have several options:

   - You can exit to DOS and perform other tasks on the server:

     a. Use the Cursor keys to highlight **Exit to the Operating System** on the Main Selection Menu.

     b. Press Enter.

        Result: The DOS prompt appears.

        Note: To redisplay the server's Main Selection Menu, type MENU at the DOS prompt, and press Enter.

   - You can reinvoke the user interface to access the background processes:

     a. Use the Cursor keys to highlight the monitor application on the Main Selection Menu.

     b. Press Enter.

        Result: The Monitor Services Menu appears (Figure 4–17).

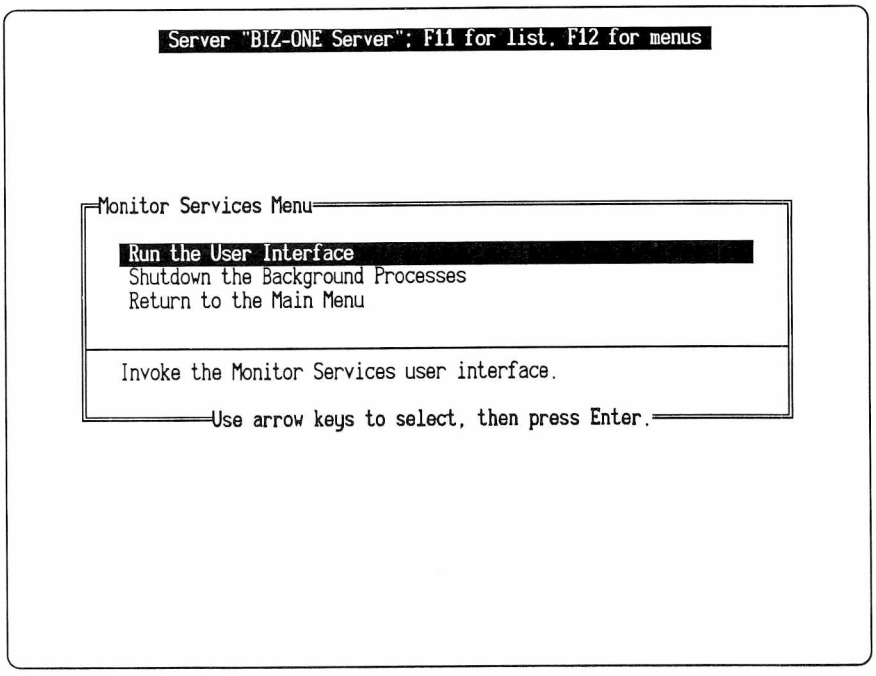


Figure 4–17. Monitor Services Menu.

c. Use the Cursor keys to highlight **Run the User Interface**.

d. Press Enter.

Result: The monitor server's Main Menu appears.

- You can shut down the background processes:

a. Use the Cursor keys to highlight the monitor application on the Main Selection Menu.

b. Press Enter.

Result: The Monitor Services Menu appears (Figure 4–17).

c. Use the Cursor keys to highlight **Shutdown the Background Processes**.

d. Press Enter.

Result: You are prompted as to whether or not you want to shut down the monitor.

e. Press "y" for "yes," and then press Enter.

To enable the Autoconnect function and to specify a time interval between connection attempts:

1. On the console's Main Menu, move the highlight to the **Options** item.
2. Use the Cursor Right key to move the highlight to the **Options** menu.
3. Use the Cursor Up key to move the highlight to the **Autoconnect** item.
4. Press the Spacebar to change the x to check (√).

   Note: **Autoconnect** will skip any server that requires a password to log on.
5. With the highlight on the **Autoconnect** item, use the Cursor Right key to move to the **Interval** item (Figure 4–18).

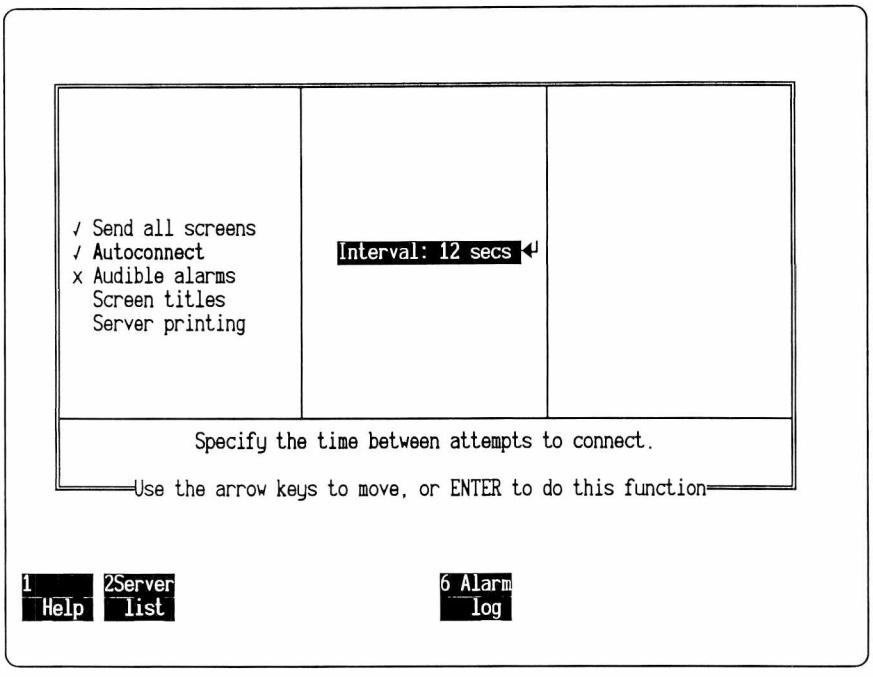


Figure 4–18. Autoconnect menu.

6. Press the Enter key.

   Result: The Enter Value dialog box (Figure 4–19) appears.

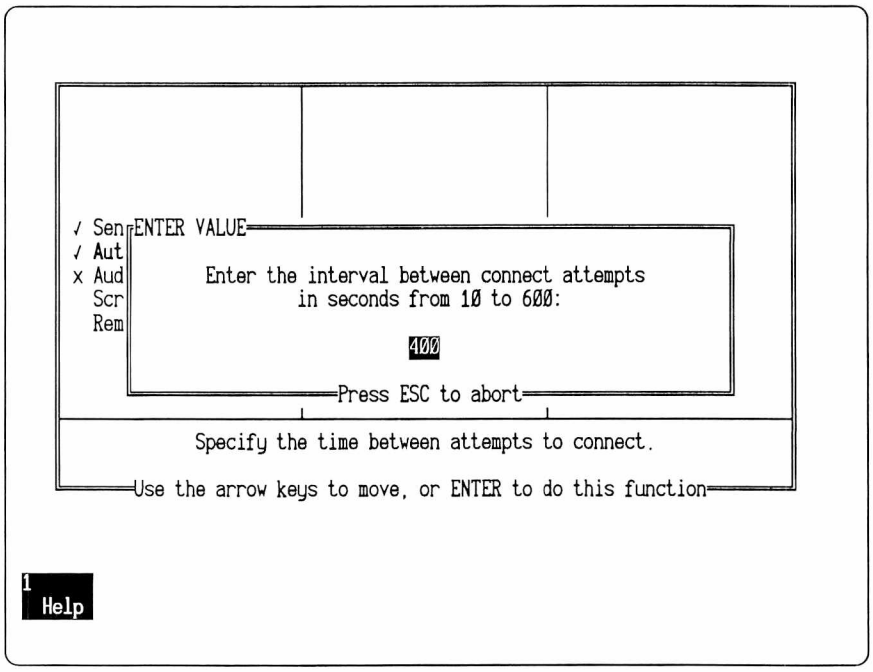


Figure 4–19. Enter Value dialog box for **Autoconnect**.

7. Type in an interval between 10 and 600 seconds.

8. Press Enter.

To display screens of multiple, connected Sniffer servers on a carousel:

1. Press F9 (**Screen carousel**).

   Note: For more information on the formatting and operation of the screen carousel, see "Screen Carousel" on page 4–39.

2. Stop the carousel at any time by striking any key.

   Result: You can control the Sniffer server visible on the carousel using the SniffMaster console keyboard. The Sniffer server will now accept keystrokes from the console. Refer to the appropriate manual(s) for further information:

   - *Distributed Sniffer System: Analyzer Operations Manual*
   - *Distributed Sniffer System: Token Ring Monitor Operations Manual*
   - *Distributed Sniffer System: Ethernet Monitor Operations Manual*

3. Press F11 (**Next**) to resume the carousel.

Using Server Information on the Server Status Display

Besides controlling servers, the Server Status display provides concise, valuable information about servers under the control of the console. There are three types of information for every server known to a particular console:

- Current status
- Monitor's alarm
- Messages exchanged between the server and the console.

This section describes "Current status" and "Monitor's alarm" and how to use them.

Current Status of a Server

Figure 4–20 provides examples of all three types of server information: Current Status, Monitor's Alarm, and Messages Exchanged.

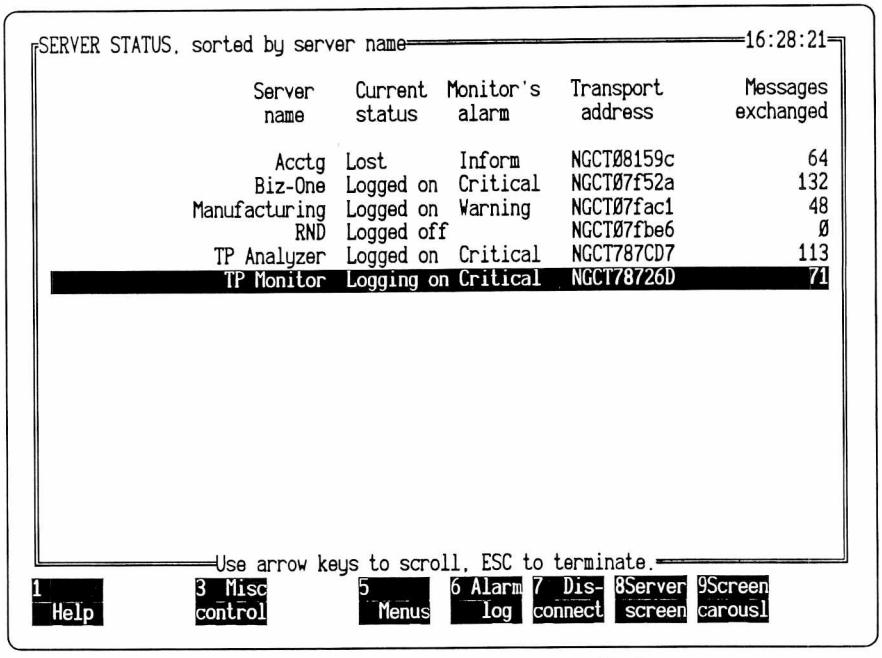


Figure 4–20. Server information in Server Status display.

The Current Status column contains four different indicators of the status of different servers: "Lost," "Logged on," Logged off," and "Logging on." The server, "Biz-One," is "Logged on" which means that it is now connected and you can view its screens at any time. The server, "Acctg," is "Lost." This means that the server was disconnected somehow and that the console did not receive a proper "Logged off" message, for whatever reason. Theoretically, you could highlight "Acctg" again, and press F7 (**Connect**) to try to recover the connection. The indicator, "Logging on," appears when you've enabled **Autoconnect**, and the server is attempting to connect to that server.

Monitor's Alarm Level

The Monitor's Alarm column tells you the "state" of each server as registered on the Server Status display. In Figure 4–20 the server, "Biz-One," is in a "Critical" state, whereas "Acctg" is only in an "Inform" state. A server's state is the highest level, unacknowledged alarm that the server has sent. This provides a simple and direct indication of how severe a situation is on a particular network.

Acknowledging Alarms at the Server. Acknowledging all alarms in a server's alarm log that are the highest level alarms sent by that server will change the state of that server. For example, if there is a "critical" alarm registered on the server's alarm log and an "inform" alarm, acknowledging the "critical" alarm will change the server's state to "inform." This change of state will show up in the console's Server Status display. This lets you keep the alarm listed on the Alarm

Log of the server and keep the state of the server as indicated in the Monitor's Alarm column of the Server Status display up to date.

Acknowledging Alarms at the Console. You can also acknowledge alarms in the console's Alarm Log, however, there is no connection between this and acknowledging alarms at the server. By acknowledging an alarm in the console's Alarm Log, a ✓ appears in the Ack column and the audible alarm beeps will change to reflect the highest unacknowledged alarm in the console's Alarm Log. For more information, see "Alarm Log" on page 4–46.

The following procedure explains how to acknowledge an alarm at a server so you can keep the Monitor's Alarm column, as registered on the console's Server Status display, up to date:

To acknowledge a server's alarm and to update the Monitor's Alarm level on the console:

1. At the console's Main Menu, highlight **Control servers**.
2. Press Enter. Alternatively, press F2 (**Server list**).
3. Use the Cursor keys to highlight the server whose Alarm Log you want to update:
   - If its Current Status is "Logged on" press Enter. Alternatively, press F8 (**Server screen**).
   - If its Current Status is "Logged off" or "Lost," press F7 (**Connect**) first, and then press Enter.

   Result: The server's screen appears.
4. Use the Cursor keys to highlight **Alarm log** in the Display menu of the server.

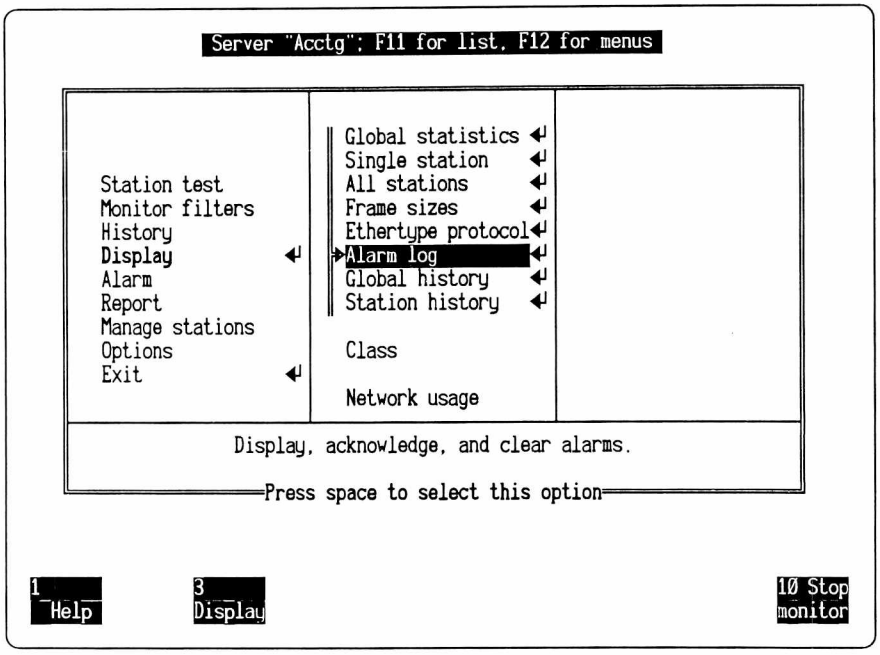


Figure 4–21. **Alarm log** *option on a server's Display menu.*

5. Press the Spacebar.

   Result: The pointer moves to indicate that the Alarm Log view is selected (Figure 4–21).

6. Press Enter.

   Result: The server's Alarm Log view appears.

7. Highlight a high level alarm you want to acknowledge in the server's Alarm Log.

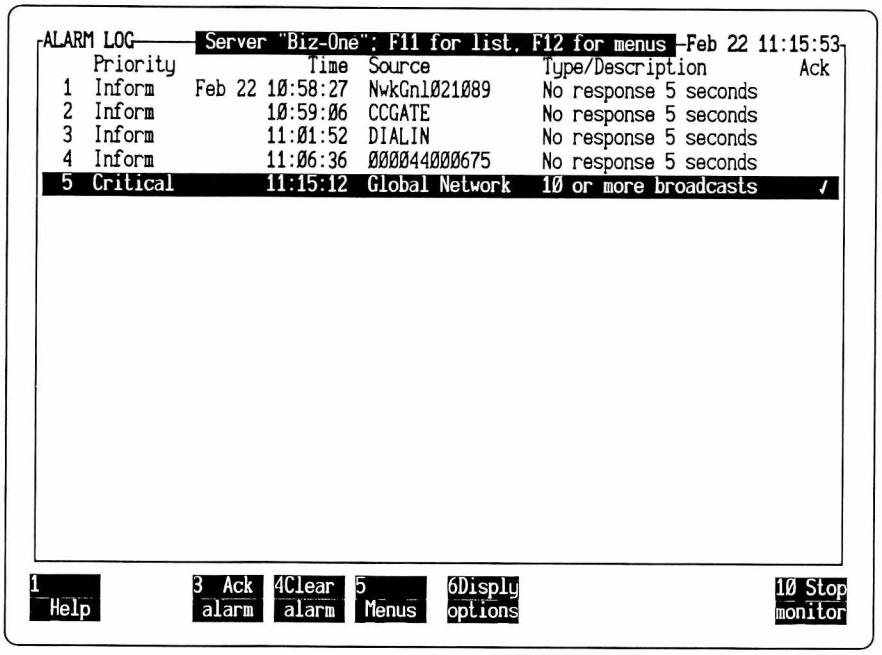


Figure 4–22. Acknowledging an alarm in a server's Alarm Log.

8. Press F3 (**Ack alarm**).
9. Repeat for other high level alarms.

   Result: In the Ack column of the server's Alarm Log, a ✓ appears next to the alarm message (Figure 4–22). In the console's Server Status display, the console will change the server's state to the highest level, unacknowledged alarm it has received from that server.

Miscellaneous Control

The **Server Status** display provides another set of control functions of the Sniffer servers. These let you:

- Transfer files from the Sniffer server to the SniffMaster console.
- Transfer files from the SniffMaster console to the Sniffer server.
- Update Sniffer server software.
- Reboot the Sniffer server.

Transfer is the key function for helping you backup critical files on each server. For specific instructions about using the transfer function to back up, see "To restore files from a backup to the hard disk if the hard disk is functioning and has DOS installed on it:" on page 2–15.

To set up a server and the console to transfer files:

1. In the Server Status display, use the Cursor keys to highlight the Sniffer server with which you want to exchange files.
2. Press F8 (**Server screen**) to view the Sniffer server.
3. Use the Cursor keys to highlight the **File Transfer Utility** item on the Main Selection Menu (Figure 4–23).

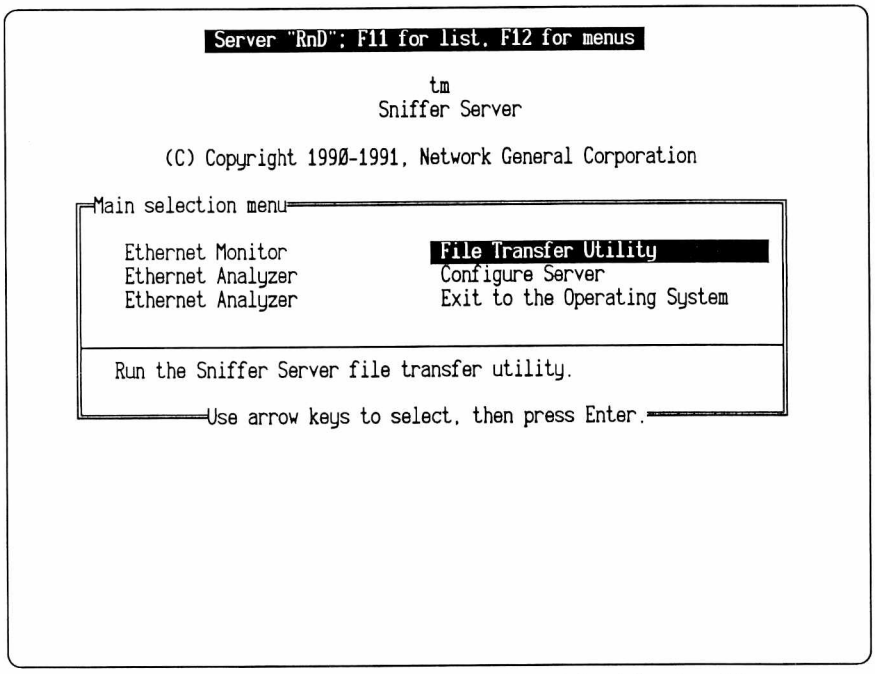


Figure 4–23. File Transfer Utility item on the Main Selection Menu.

- If the analyzer or monitor application is running, you must exit the application to the Main Selection Menu.
- If the Sniffer server is at the DOS prompt, you can type MENU at the prompt, and press Enter.

4. Press Enter.

   Result: The Sniffer server will install the Server File Transfer Utility.

   Note: This is the condition in which you must leave the Sniffer server in order carry out any transfer. Press the Esc key to terminate the file transfer utility.

5. Press F11 (**List**) to return to the Server Status display.
6. Highlight the desired server on the list.
7. Press F3 (**Miscellaneous control**).

Result: The Miscellaneous Control menu with the name of the Sniffer server in the upper left-hand corner appears (Figure 4–24).

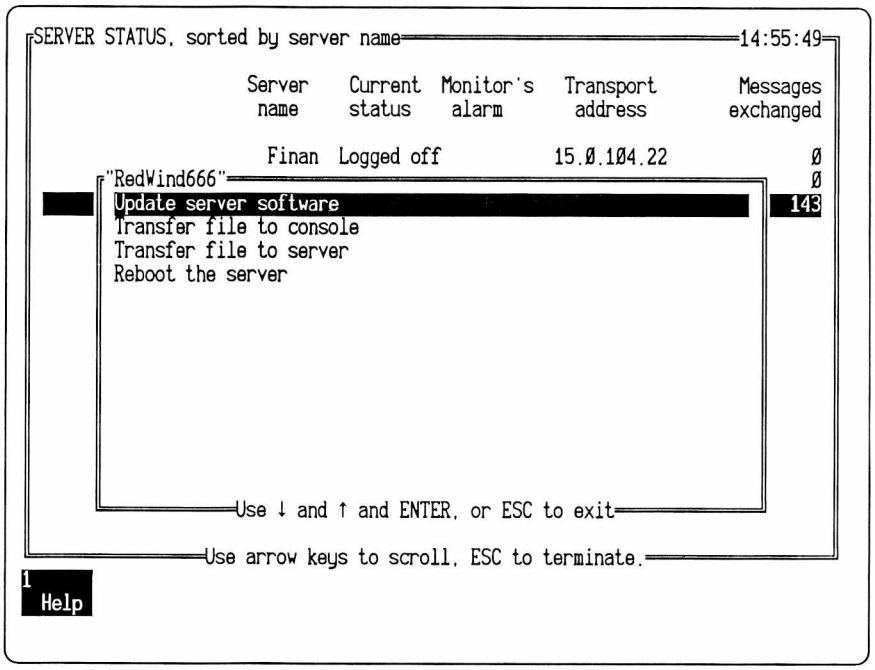


Figure 4–24. Miscellaneous Controls menu.

To transfer a file from a Sniffer server to the SniffMaster console:

1. Make certain that the File Transfer Utility is running.
2. On the Miscellaneous Control menu, use the Cursor keys to move the highlight to the item, **Transfer file to console**.
3. Press Enter.

   Result: The field for entering the source filename appears.
4. Type in the source filename on the Sniffer server.
5. Press Enter.

   Result: The field for entering the destination filename appears.
6. Type in the destination filename on the SniffMaster console.
7. Press Enter.

   Result: The message, "Uploading [filename]," appears during the transfer process.

   You may get one of several messages after the transfer process. See the table in Figure 4–25 for information on their meaning and further user actions.

Message	User Action
"Transfer completed"	Press any key to return to the **Miscellaneous Controls** menu.
"Timeout"	Try again. Increase the "timeout" value at the server.
"Transfer failed at the console–file not found"	Wrong path or filename. You must specify the console drive.
"Transfer failed at the console–network timed out"	File Transfer Utility not installed. Go to Server's Main Selection Menu.

Figure 4–25. Messages and user action during file transfer.

The File Transfer Utility is still loaded at the Sniffer server. To terminate the File Transfer Utility when you are finished, return to the server, and press the Esc key.

To transfer a file from the SniffMaster console to a Sniffer server:

1. Make certain that the File Transfer Utility is running.
2. On the Miscellaneous Control menu, use the Cursor keys to move the highlight to the item, **Transfer file to server**.
3. Press Enter.

   Result: The field for entering the source filename appears.
4. Type in the source filename on the SniffMaster console.
5. Press Enter.

   Result: The field for entering the destination filename appears.
6. Type in the destination filename on the Sniffer server.
7. Press Enter.

   Result: The message, "Downloading [filename]," appears during the transfer process (Figure 4–26).

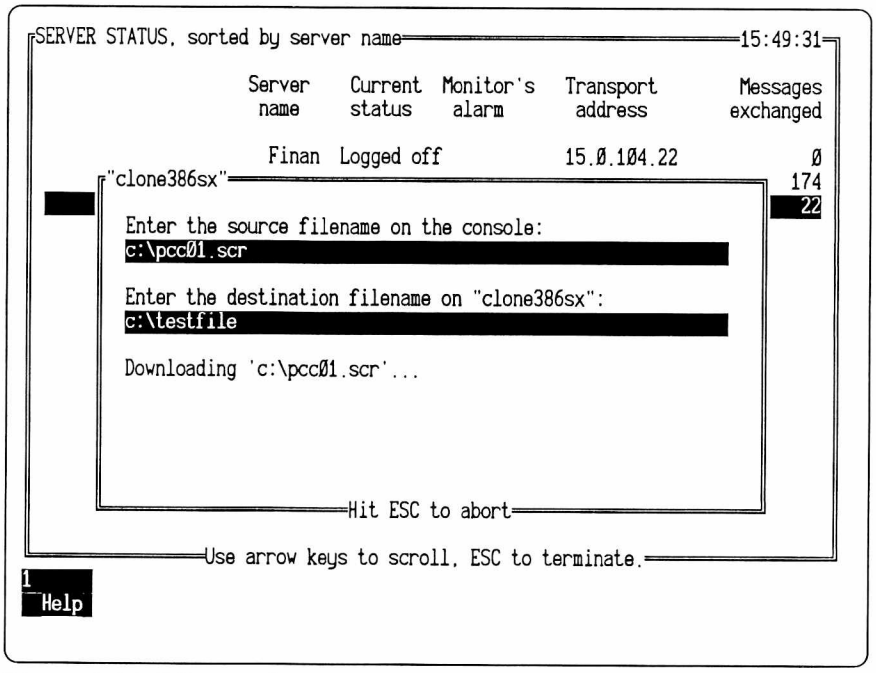


Figure 4–26. File transfer using Miscellaneous Control.

You may get one of several messages after the download process. See the table in Figure 4–25 for information on their meaning and further user actions.

The File Transfer Utility is still loaded at the Sniffer server. To terminate the File Transfer Utility when you are finished, return to the server. and press the Esc key.

To update Sniffer server software:

1. Read the detailed instructions that accompanied your update diskettes.

   Note: You must follow these instructions. What is described in this procedure is a general overview of the process.

2. Update the console software.

   Note: The order in which you update console and server software may change in the future. For the foreseeable future, you will update the console software first.

3. Exit the console application to the DOS prompt.

4. Load the server update software onto the console's hard disk.

   Note: You can load multiple sets of server update software onto one console and then update different types of servers from the same console.

5. Start the console application.

6. Connect to the server to be updated.
7. Terminate any application running on the server, and exit to the server's Main Selection Menu.
8. Invoke the File Transfer Utility from the server's Main Selection Menu.
9. Return to the Server Status display on the console.
10. Press F3 (**Miscellaneous Control**).
11. On the Miscellaneous Control menu, use the Cursor keys to highlight to the item, **Update server software** (Figure 4–24).
12. Press the Enter key.

    Result: The console proceeds to download all new files. When errors are encountered during the process, following the suggestions to resolve the error condition.
13. Select the Reboot server option from the Miscellaneous Control menu.

    Result: The new software takes effect after the reboot.

The File Transfer Utility is still loaded at the Sniffer server. To terminate the File Transfer Utility when you are finished, return to the server, and press the Esc key.

To reboot a Sniffer server from the console:

1. Open the Server Status display.
2. Press F3 (**Miscellaneous control**).
3. On the Miscellaneous Controls menu, use the Cursor keys to move the highlight to the item, **Reboot the server.**
4. Press the Enter key.

   Result: A confirmation window appears. The console will disconnect the Sniffer server and reboot it. Do you have **Autoconnect** turned on?

   - If you have **Autoconnect** turned on and there is no specified password, the console will reconnect for you.
   - If you do not have **Autoconnect** turned on, the console will redisplay the Server Status window with the server highlighted.

System Information Output

The SniffMaster console has several ways that it presents information about your system. One is visual output that you see on the console's display. A second is auditory output that you hear coming from the console. Finally, there is printed output that you can direct to and from a variety of sources and destinations.

Visual Information

This section discusses how the SniffMaster console presents visual information about your network in two forms:

- Screen carousel
- Alarm log

The screen carousel lets you work with your connected servers, individually or collectively. It lets you see what they see and control them to do your bidding. The Alarm Log lists all alarms sent to the console from connected Sniffer monitor servers. This provides you with one place to look for threshold events that trigger alarms on the different segments, rings, and links. For both of these forms, you have various options for formatting the displays to make the system information more useful and readable to you.

Screen Carousel

The screen carousel is a continuously rotating display of the screens of all Sniffer servers currently logged on. You must have more than one server logged on. Once started, the carousel will rotate automatically at a speed you select or manually as you press a function key. You can pause the carousel at any of the servers displayed on the carousel, resume the carousel, backtrack to previously displayed server screens, return to the Server List, or return to the console's Main Menu.

This section covers three main topics:

- How to start the screen carousel.
- How to control the screen carousel.
- How to configure the screen carousel using SniffMaster console menus.

Starting the Screen Carousel

To start the screen carousel after logging on servers:

1. Use the Cursor keys to highlight the **Screen carousel** item on the Main Menu (Figure 4–27).

2. Press Enter, or, alternatively, press F9 (**Screen carousel**).

   Note: When one or more Sniffer servers are logged on, F9 (**Screen carousel**) is active when you are working in any of the console menus, the Server Status screen, or the Alarm Log.

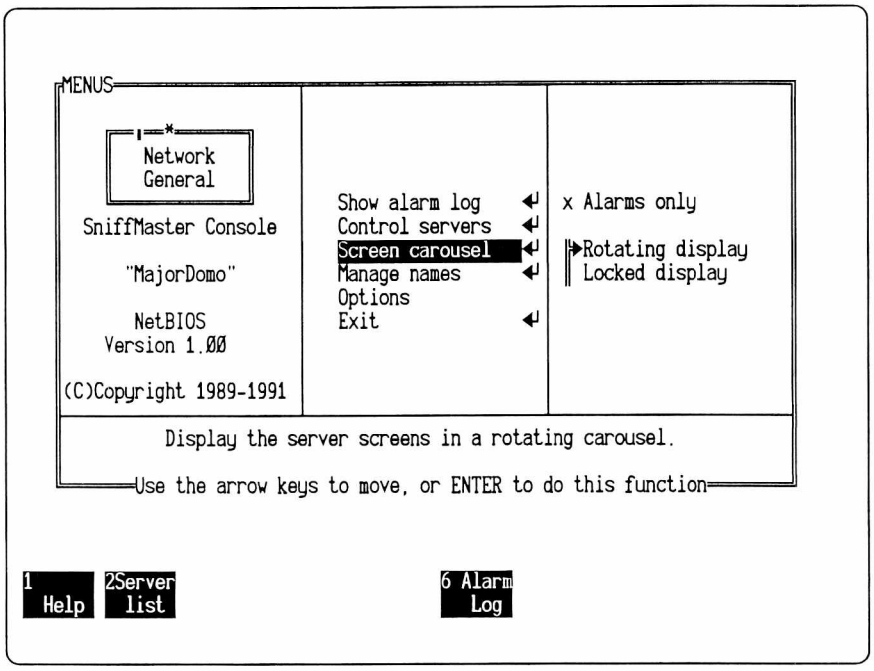


Figure 4–27. **Screen carousel** *item on the Main Menu.*

Result: Look for menus or screens from logged on servers.

Figure 4–28 shows an example of a server screen as displayed on the console. Note the distinctive screen title at the top that provides the name of the server as well as a small menu reminding you of active console function keys. Figure 4–28 shows a screen from a Sniffer server monitoring a network.

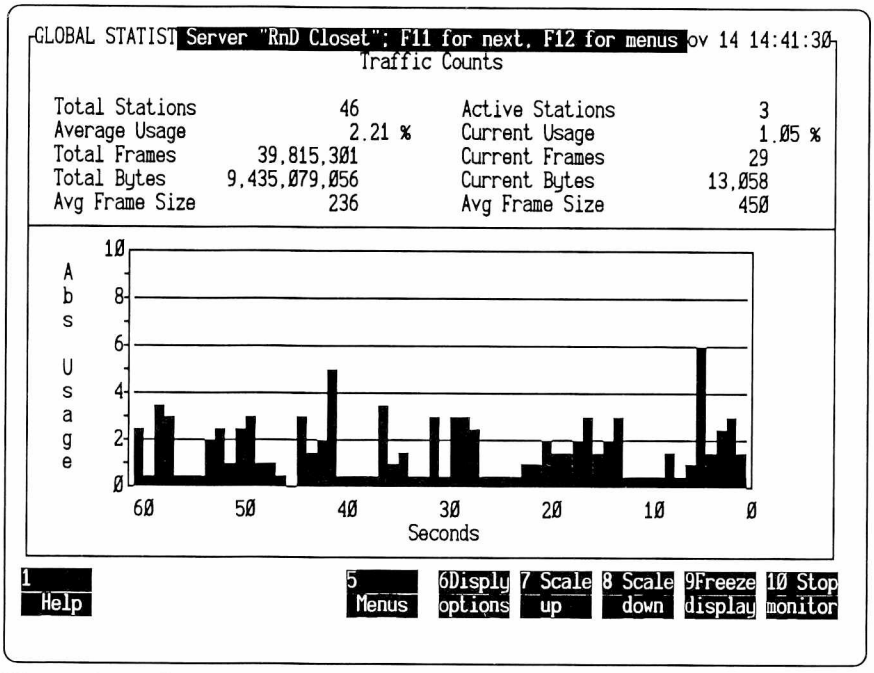


Figure 4–28. Screen carousel display on the SniffMaster console.

You can now control any of the servers passing by on the carousel. Most keystrokes you make at this time at the console's keyboard will be passed to the server. Refer to the appropriate manual(s) for further information:

Distributed Sniffer System: Analyzer Operations Manual

Distributed Sniffer System: Token Ring Monitor Operations Manual

Distributed Sniffer System: Ethernet Monitor Operations Manual

Controlling the Screen Carousel

There are a few keys reserved for controlling the SniffMaster console itself. At the top of the screen you can see a small SniffMaster console menu. It indicates two of the possible controls you can have over the carousel. With the carousel running, you have several controls available. You can:

- Pause the carousel
- Advance to the next server screen
- Backtrack to the previous server screen
- Return to the SniffMaster console Main Menu

To control the screen carousel:

1. While the carousel is rotating, you can pause the rotation at any time:

   a. Press any key.

      Note: At this point, you can control the server whose screen is on the console's display. Most keys you press will be communicated to the remote server.

2. When you've paused the carousel, you can advance to the next server screen on the carousel:

   a. Press F11 (**Next**).

      Note: You may use this when you do not want to wait for the rotation interval of a rotating display or when you selected a locked display.

3. When necessary, you can backtrack to the previous server screen on the carousel:

   a. Press Shift-F11.

      Note: Pressing Shift-F11 repeatedly will, in effect, reverse servers' order of appearance on the carousel.

4. When you are ready, you can return to the SniffMaster console Main Menu:

   a. Press F12 (**Menus**).

Formatting the Screen Carousel Display

The default display for the SniffMaster console may not entirely meet your requirements for usefulness or readability. You have several options for enhancing the display. From SniffMaster console menus (Figure 4–27 and Figure 4–29), you can control:

- Whether or not to show only logged-on Sniffer servers that have alarms.
- Whether the carousel advances automatically (and at what rate) or remains locked for you to advance manually.
- Which of several visual techniques should be used to change from one screen to another and what transition interval.
- Where and how you want the SniffMaster console screen title to appear when viewing server screens.

To determine whether or not to show only logged-on servers with alarms:

1. Use the Cursor keys to highlight on **Screen carousel** in the Main Menu.
2. Press the Cursor Right key.
3. Use the Cursor keys to highlight the **Alarms only** menu item.
4. Press the Spacebar to enable or to disable **Alarms only**.
   - A ✓ indicates that only connected servers with alarms will show.
   - An x indicates that all connected servers will show.

To determine whether the carousel will advance automatically or manually:

1. Use the Cursor keys to highlight the **Screen carousel** item in the Main Menu.
2. Press the Cursor Right key.
3. Use the Cursor Up or the Cursor Down key to highlight either the **Rotating display** item or the **Locked display** item.
4. Press the Spacebar to select your option.

   Result: Notice that the pointer moves to indicate your choice.

To select the transition technique for the rotating display:

1. Use the Cursor keys to highlight the **Screen carousel** item in the Main Menu.
2. Press the Cursor Right key.
3. Press the Cursor Right key again.
4. Use the Cursor Up or the Cursor Down key to highlight the option you want (Figure 4–29).

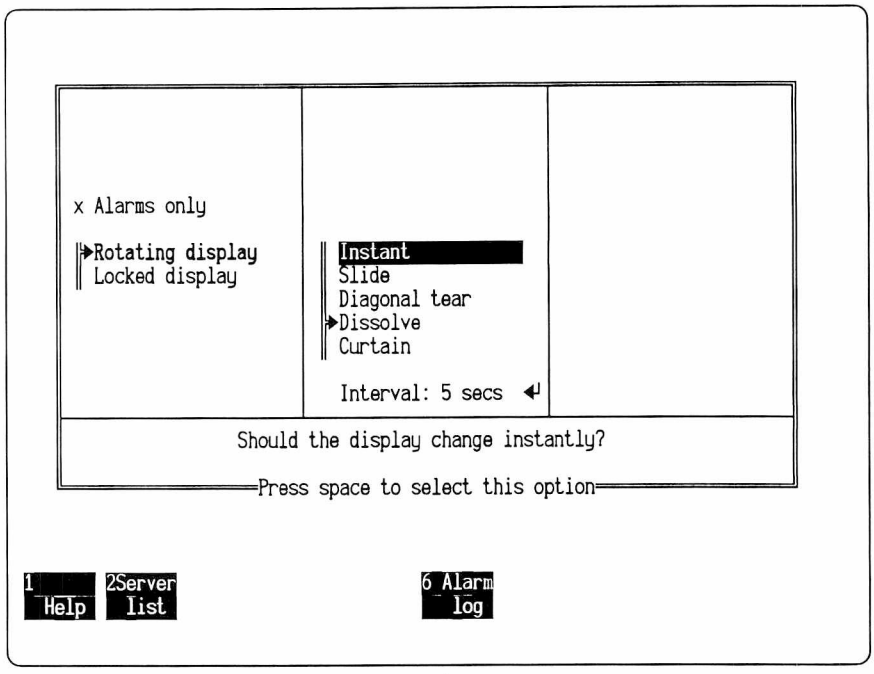


Figure 4–29. Carousel \ Rotating Display menu.

5. With the highlight on the option you want, press the Spacebar.

   Result: The pointer moves to indicate your selection.

   Note: There are five options for the visual transition effect from one Sniffer server screen to another. Figure 4–30 lists and describes the options. When choosing an option, consider the particular Sniffer server screens to be displayed. Some options more dramatically show the transition between certain types of server screens.

Option	Function
Instant	Sudden change from old screen to new screen.
Slide	New screen slides from right to left.
Diagonal tear	Old screen peels along several diagonal lines.
Dissolve	Old screen fades into new screen.
Curtain	New screen opens as curtain at center from center to left and right edges.

Figure 4–30. Carousel \ Rotating Display menu options.

6. Press the Spacebar to select the option.

   Result: Notice that pointer moves to indicate your choice.

To change the time interval of the rotating display transition:

1. Go to the Screen Carousel\Rotating Display menu.
2. Use the Cursor Down key to highlight the **Interval** option (Figure 4–29).
3. Press Enter.

   Result: Look for the Enter Value dialog box.
4. Type a rotation interval value between 1 and 99 seconds.
5. Press Enter.

To configure the carousel screen titles:

1. Use the Cursor keys to highlight the **Options** item in the Main Menu.
2. Press the Cursor Right key to move to the Options menu.
3. Press the Cursor Down key to highlight the **Screen titles** menu item (Figure 4–31).

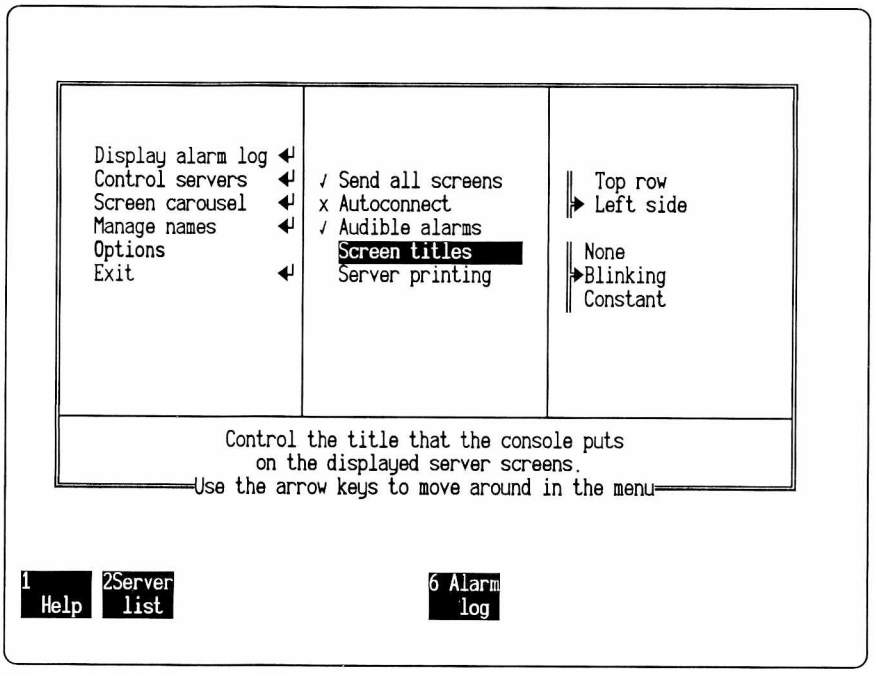


Figure 4–31. **Screen titles** *option.*

4. Press the Cursor Right key to move to the Options\Screen Titles menu.
5. Use the Cursor Up and Cursor Down keys to move the highlight to one of the two option lists on the menu.

6. Use the Cursor Up and Cursor Down keys to highlight the screen title format you want in the option list.

   Note: In the top option list, you have two choices as to the location of the screen title. The table in Figure 4–33 describes your choices.

Option	Description
Top row	Centers the screen in the very top row of the server screen. Includes console function key menu.
Left side	Centers the screen in extreme left column of the server screen. Does not include console function key menu.

Figure 4–32. Options \ Screen Titles position options.

   Note: In the bottom option list, you have three choices as to the appearance of the screen title. The table in Figure 4–33 describes the choices.

Option	Description
None	No screen title will show. Use this when the screen title interferes with reading the server screen on the console.
Blinking	Screen title flashes on and off. Use this when you want to view the screen area under the title and to be reminded of which server you are currently viewing and of which function keys are active.
Constant	Screen title remains on.

Figure 4–33. Options \ Screen Titles appearance options.

7. Press the Spacebar to select your choice.

   Result: The pointer moves to indicate your choice.

8. Repeat steps for the second option list.

Alarm Log

The Alarm Log display is a consolidated list of all alarms that have been sent to the SniffMaster console from Sniffer monitor servers logged on to it and sending alarms. When two consoles are connected to the same server, both will receive the alarms. If no console is connected to a server that is monitoring a network, and no SNMP Network Management Station is configured to receive traps, the server will simply store the alarms in its own alarm log until a console logs on. When a console does log on, all unsent alarms in the server's alarm log are sent immediately to that console. If a second console logs on to the server subsequent to the time the alarms are sent to the first console, the second console will receive only alarms that occur after it logs on.

There is a maximum to the number of alarms that can be listed at the SniffMaster console. Up to 200 alarms can be listed. When new alarms arrive at the console after the 200 maximum has been reached, the alarm log discards the "old" alarms. You can scroll through the list for alarms that are new or are unattended to, and you can prune the list by deleting unwanted messages.

Each alarm logged at the console is listed as an alarm message from a particular server. There are five parts to each alarm message:

- Name of the server sending the alarm
- Priority level of the alarm
- Time the alarm was sent according to the server's clock
- Indication of global alarm or individual offender
- Global or individual station thresholds defined at each server.

You have several ways in which you can format and control the Alarm Log display to make it more useful and readable:

- Set a filter for incoming alarms. The filter is based on priority levels, and you have five from which to choose.
- Select a criterion for sorting alarms. You can sort by five different criteria.
- Acknowledge alarms you want to keep on the list but are not ready to clear. The highest level unacknowledged alarms on the alarm list determine the audible alarm.
- Clear alarm messages from the console's list. The Alarm Log automatically eliminates the oldest alarms (alarms beyond the 200 maximum); however, you must manually delete unwanted messages or problems that have been taken care of.

Alarm information can also be automatically stored to the console's hard disk in the \CONSOLE\ALARM directory for each console session. Also, you can choose between a standard format or a comma-separated value format. The console creates one file for each day you use the console and adds the extension, .ALM. The filename is the date of the console session. For example,

```
910503.ALM
```

is the name for a file created on May 5, 1991.

Alarms are used by the console in one other way. The highest level alarm sent by a server is registered by the console in its Server Status display. This gives you a handy, concise way of seeing the conditions that the server has seen. If that alarm is not acknowledged at the server, then that is called the server's "state." However, the actual alarm that causes the state need not have been sent to a console

currently viewing the server. Servers send messages containing "state" information independently of alarm messages.

For example, a server may have sent a "critical" alarm and an "inform" alarm. If both alarms are unacknowledged, then the server is defined by the console as being in a critical state. However, if the critical alarm is acknowledged at the server and the inform alarm is not, then the server is defined by the console as being in an inform state. This is useful when you want to keep alarms listed in a server's Alarm Log but no longer want that alarm to affect the server's state. For more information, see "Using Server Information on the Server Status Display" on page 4–29.

Using the Alarm Log

This section covers procedures and guidelines for displaying the alarm log and for interpreting the alarm messages sent by servers logged on to the console. Each message has five elements to it: Server Name, Alarm priority, Alarm Timestamp, Offender, and Alarm Type Description.

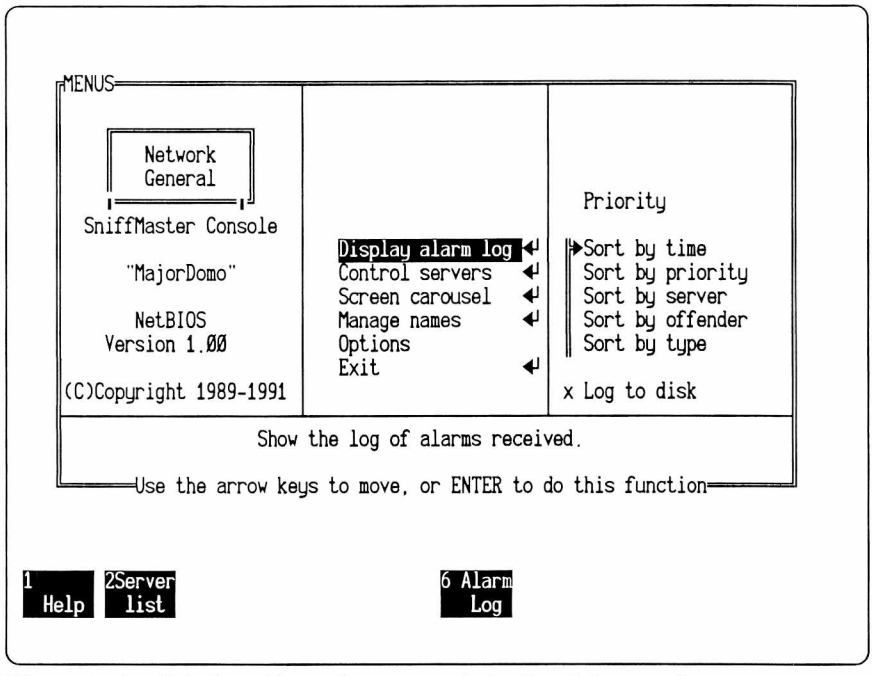


Figure 4–34. Display Alarm Log menu is in the right panel.

To display and to read the Alarm Log:

9. Use the Cursor keys to highlight **Display alarm log** in the Main Menu (Figure 4–34), press the Enter key. Alternatively, you can press F6 (**Alarm log**).

   Result: The Alarm Log display appears (Figure 4–35).

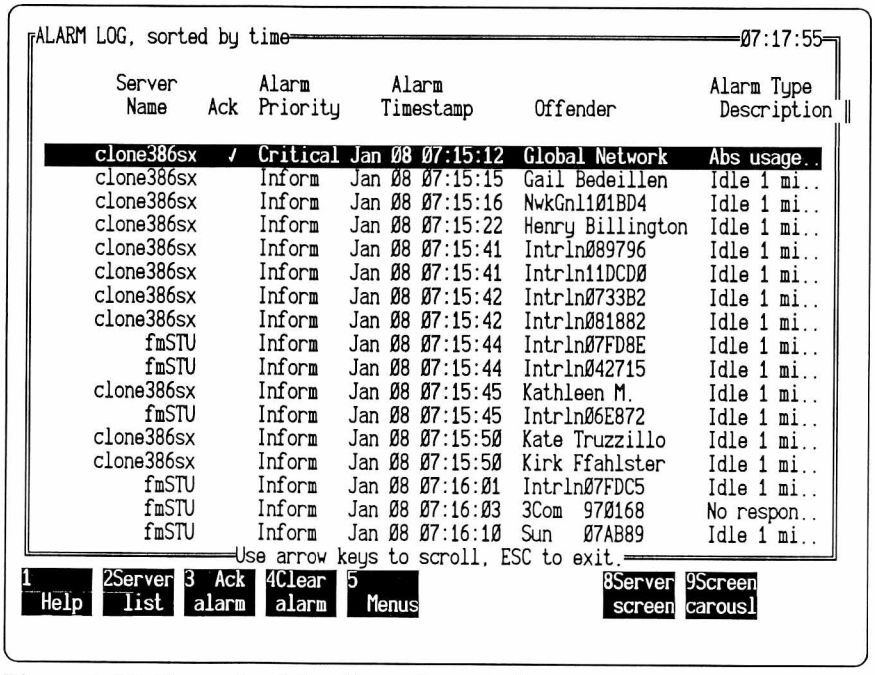


Figure 4–35. Example of the Alarm Log window.

Figure 4–35 shows an example of the Alarm Log window. There are six columns containing information about the alarms logged at the console. The table in Figure 4–36 lists the titles and contents of the columns in the Alarm Log.

Column Title	Column Content
Server Name	Name assigned to server with **Manage names** on Main Menu.
Ack	Acknowledgement. Pressing F3 (**Ack Alarm**) puts a ✓ in the column. The highest level unacknowledged alarms determine the audible alarm level.
Alarm Priority	The severity level of the alarm message. You set individual station alarm levels at each server. All Global Network alarms are "Critical" by default. The highest level listed in this column determines the audible alarm currently sounding on the console.
Alarm Timestamp	Date and time the alarm occurred.
Offender	Indicates an individual station alarm or a global alarm by listing name or address of individual station triggering alarm or by posting "Global Network." If "Unknown Station," this is a global alarm and gives name and address of unknown station.
Alarm Type Description	Global and individual station thresholds defined at each monitor. For more information, see the table in Figure 4–37.

Figure 4–36. Column titles and contents for the Alarm Log.

The table in Figure 4–37 describes the various types of alarms that appear in the Alarm Description column. You set the thresholds for alarms at each server for the network it monitors and for each station on that network.

Category	Type	Description
Individual Station	Errors	Number of bad frames (on Ethernet) or soft error report frames (on token ring) a station can transmit on the network before triggering an alarm.
	No response	Length of time a station can be sent frames without responding before triggering an alarm.
	Idle	Length of time a station can go without transmitting before triggering an alarm.
	Usage	Percentage of relative network traffic a station can generate before triggering an alarm.
	Oversized frame	One or more frames exceeding 4,608 bytes on 4 Mb/s or 18,432 on 16 Mb/s token ring. On Ethernet, the limit is 1,514 bytes.
	Beacon	A station detected a hard error that renders a token ring network inoperable.
	Ring poll failure	An error occurred during a token ring poll process; notice sent by active monitor.
Global	Unknown station	Address not found in address table triggering an alarm.
	Errors	Number of bad frames (on Ethernet) or soft error report frames (on token ring) on network triggering an alarm.
	Usage	Percentage of absolute network usage before triggering an alarm.
	Broadcast	Number of frames that can be sent to the broadcast address before triggering an alarm.
	Idle	Length of time the network can be inactive before triggering an alarm.
Other	Illegal source address	The source address of an otherwise good Ethernet frame is given as a broadcast address.

Figure 4–37. Types of errors appearing in the Alarm Description column.

For detailed information about these types of errors and the default thresholds, see the relevant manual:

- *Distributed Sniffer System: Ethernet Monitor Operations Manual*
- *Distributed Sniffer System: Token Ring Monitor Operations Manual*

Formatting the Alarm Log Display

This section describes procedures for formatting the Alarm Log to make it more useful for your particular system. These procedures will show you how to:

- Set a filter for alarms of different priority levels sent by servers. You can set a filter to include from one to five levels: Inform, Warning, Minor, Major, and Critical.
- Select a criterion for sorting Alarm Log messages. You can elect to sort the alarm messages by time, priority, server, offender, and type. You have five types of alarms from which to choose. The types represent a range of severity or an order of importance. **Inform** is the least severe and important; **Critical** is the most severe and important. Global network alarms are all of **Critical** priority by default, and this cannot be changed. Four other specific alarms are **Critical** by default, and you cannot change them: Oversized frames, Beacon, Ring poll failure, and Illegal source address.

  Alarms sent by the servers are listed on the console's consolidated alarm log if their priority level is selected. The default is that all priority levels are selected. You set the alarm levels for individual stations at the network monitoring server.
- Clear an alarm message from the Alarm Log list. You can delete alarm messages you don't want listed any more.

To set a filter for incoming alarm priority levels:

1. Use the Cursor keys to highlight the **Display alarm log** item in the Main Menu.
2. Press the Cursor Right key to move the highlight to the Display Alarm Log menu.
3. Press the Cursor Up key to move the highlight to the **Priority** item.
4. Press the Cursor Right key to move the highlight to the Display Alarm Log\Priority menu (Figure 4–38).

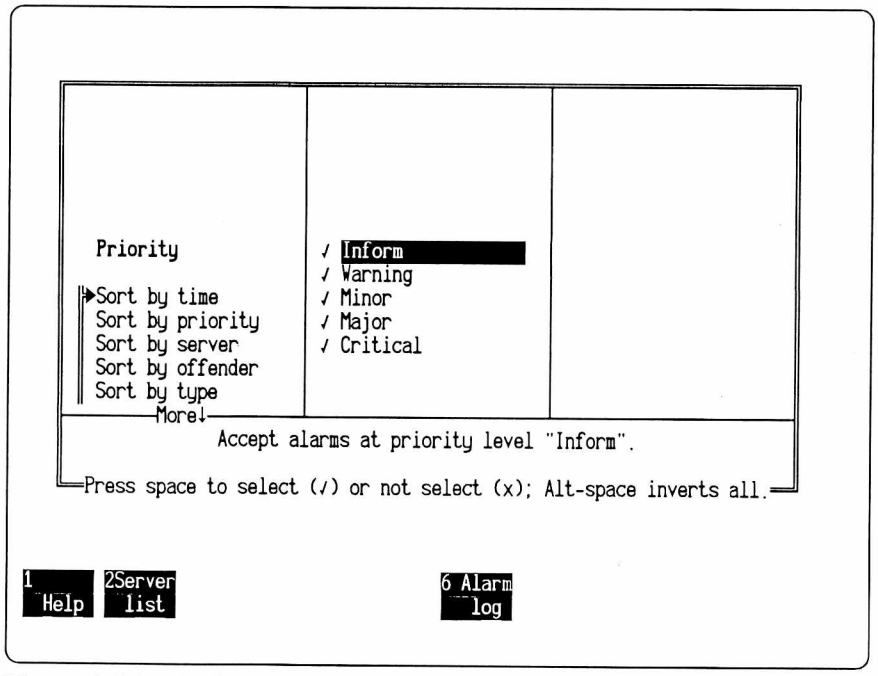


Figure 4–38. Display Alarm log \ Priority menu.

5. Use the Cursor Up and the Cursor Down keys to highlight each type of alarm you want included in the Alarm Log display: Inform, Warning, Minor, Major, and Critical.

   Note: The selection you make here will also affect the audible alarm. See the section, "Auditory Information" on page 4–56.

6. Press the Spacebar.

   Result: An x to the left of the priority level indicates that the level will be excluded. A ✓ indicates that it will be included.

To select a criterion for sorting alarm messages in the Alarm Log:

1. Use the Cursor keys to highlight **Display alarm log** on the Main Menu.
2. Press the Cursor Right key to move the highlight to the Display Alarm Log menu.
3. Use the Cursor Up and the Cursor Down keys to highlight the criterion you want to sort the Alarm Log by (Figure 4–39).
4. Press the Spacebar.

   Result: The pointer moves to indicate your choice.

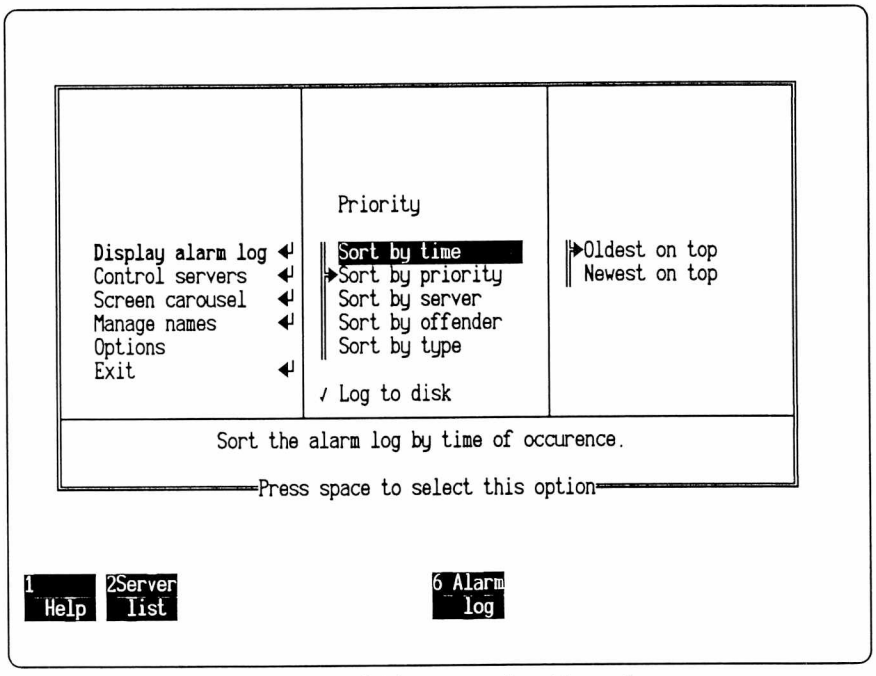


Figure 4–39. Five criteria by which to sort the Alarm Log.

To clear an alarm message from the Alarm Log list:

1. Use the Cursor keys to highlight the **Display alarm log** item on the Main Menu.
2. Press Enter or, alternatively, press F6 (**Alarm log**).

   Result: The Alarm Log display appears.
3. Use the Cursor Up and the Cursor Down keys to highlight the message you want to remove.
4. Press F4 (**Clear alarm**).

   Result: The alarm message disappears.

Storing Alarm Information on Disk

You can automatically save alarm information to preserve it for each console session. There will be one file for each day. Each file is located in the \CONSOLE\ALARM directory. The filename will be of the form *yymmdd.ALM*. For example,

```
910605.ALM
```

is the name of a file created on June 5, 1991. Old alarm files should be removed manually from time to time or eventually the disk will fill up.

In addition to storing the alarm information, you can also determine the file format in advance. You can choose between the delimited format or the standard format:

- **Delimited format.** Allows you to import the file into other applications, such as spreadsheets and databases. The format contains no page breaks or embedded commas with fields.
- **Standard format.** Numbers that are 1,000 or greater have embedded commas within fields.

To log alarm message information to disk:

1. Use the Cursor keys to highlight the **Display alarm log** item in the Main Menu.
2. Press the Cursor Right key to move the highlight to the Display Alarm Log menu.
3. Press the Cursor Down key to move to highlight the **Log to disk** item (Figure 4–40).

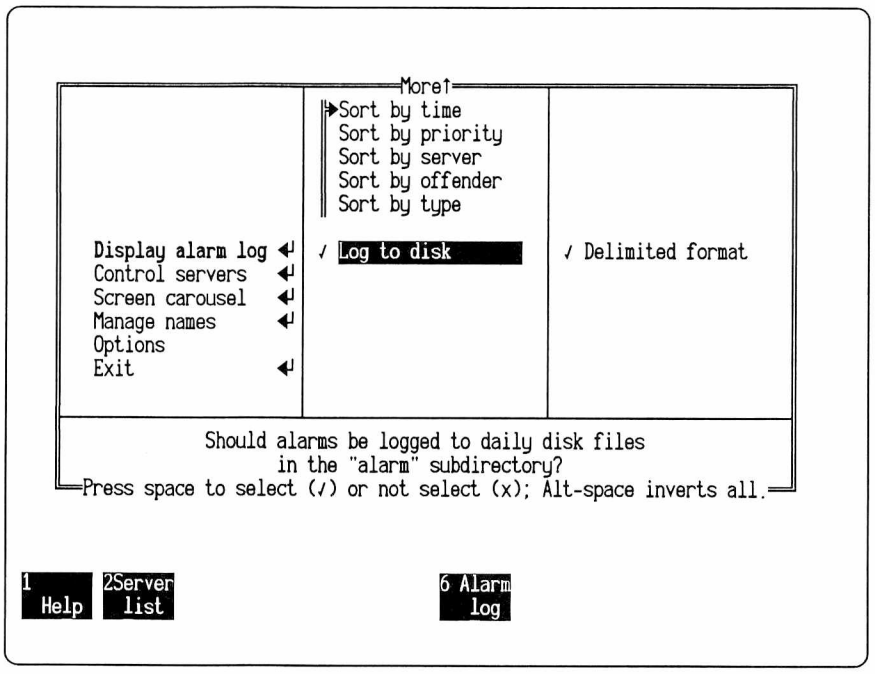


Figure 4–40. **Log to disk** *option.*

4. Press the Spacebar to change the x to a ✓ and to enable **Log to disk**.

To select a file format:

1. Use the Cursor keys to move to the Display Alarm log\Log to Disk menu (Figure 4–41).

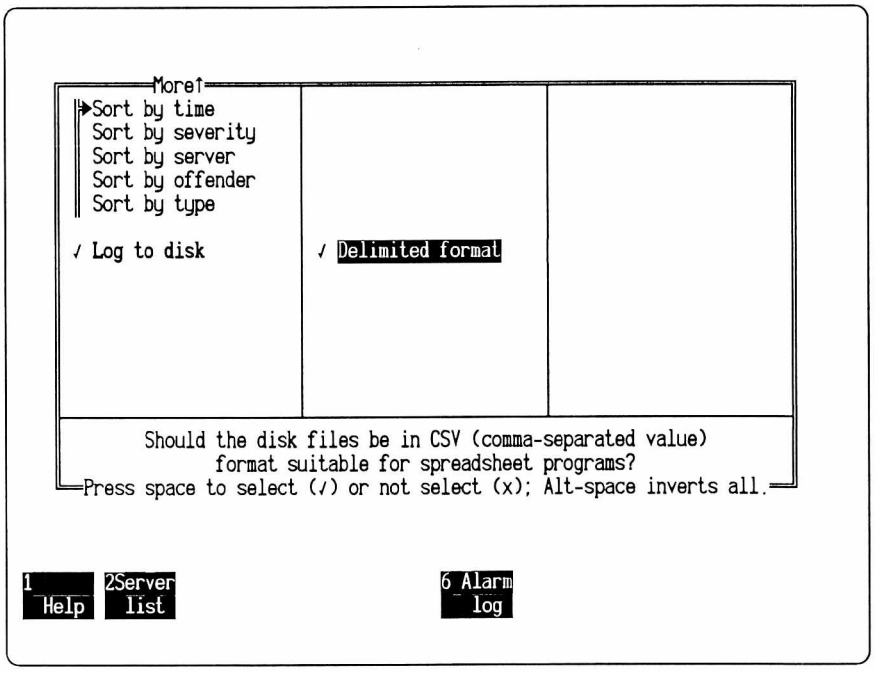


Figure 4–41. Selecting file format.

2. Press the Spacebar to choose a file format:
   - To choose the delimited format, change the x to a ✓.
   - To choose the normal file format, change the ✓ to a x.

Auditory Information

The SniffMaster console gives you auditory information, in addition to visual information, about your system. This frees you from having to look at the screen to know when important events occur. You can direct your visual attention to other tasks and let the console signal you with a sound when it has found or done something for you.

There are two basic sets of sounds. One set alerts you when the console connects to a server and when it disconnects, regardless of whether you connect or disconnect manually or via the **Autoconnect** option.

Connecting	Succession of tones with ascending pitch.
Disconnecting	Succession of tones with descending pitch.

The second set of sounds alert you to alarms as they occur. The sounds indicate the alarm priority level of the highest alarm still in the Alarm Log. The lowest priority level is Inform; the highest level is Critical. The alarm sounds are differentiated by pitch and by the number of tones before a distinct pause: the higher the priority level, the higher the pitch and the more tones.

Inform	one tone, lowest pitch
Warning	two tones, higher pitch
Minor	three tones, higher pitch
Major	four tones, higher pitch
Critical	five tones, highest pitch.

If you set a filter for different priority levels (see "To set a filter for incoming alarm priority levels:" on page 4–52), then that will affect which alarms you will hear and which alarms will be listed in the Alarm Log.

The procedures described in this section show you how to:

- Turn all sounds on and off.
- Turn sounds for connection and disconnection on and off.
- Turn Alarm Log sound on and off. The sound represents the highest priority level alarm in the console's Alarm Log.
- Select the lowest priority level alarm listed in the Alarm Log that will produce a sound.

To enable the sounds option:

1. Use the Cursor keys to move the highlight to the **Options** item on the Main Menu.
2. Press the Cursor Right key to highlight the **Audible alarms** item in the Options menu.
3. Press the Spacebar.

   Result: The x changes to a ✓.

To enable sounds for connection and disconnection:

1. Use the Cursor keys to move the highlight to the Options menu.
2. Press the Cursor Right key to move to the Options\Audible alarms menu.
3. Press the Cursor Right key to highlight **Connect/Disconnect** in the Options\Audible Alarms menu.
4. Press the Spacebar.

   Result: The x changes to a ✓.

To enable sound for the highest priority alarm posted in the Alarm Log:

1. Use the Cursor keys to move the highlight to the Options menu.
2. Press the Cursor Right key to move to the Options\Audible alarms menu.
3. Press the Cursor Down key to highlight the **Alarm log** menu item (Figure 4–42).
4. Press the Spacebar.

   Result: The x changes to a ✓.

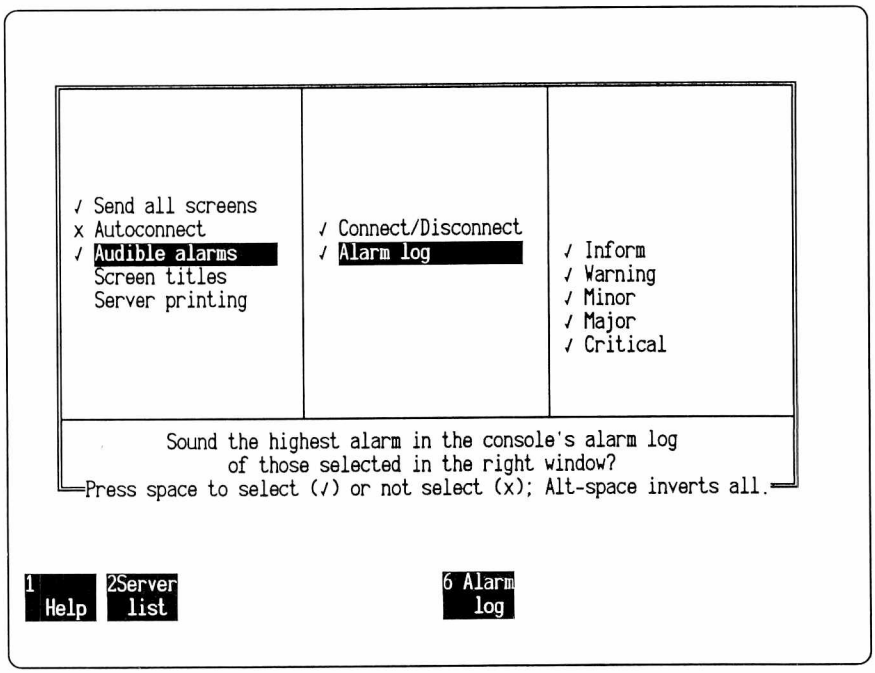


Figure 4–42. Audible Alarms menus.

To specify the highest alarm in the console's Alarm Log that will produce an audible alarm:

1. Use the Cursor keys to move the highlight to the Options menu.
2. Press the Cursor Right key to move to the Options\Audible alarms menu.
3. Press the Cursor Down key to highlight the **Alarm log** menu item.
4. Press the Cursor Right key to move to the Options\Audible Alarms\Alarm log menu.

5. Use the Cursor Down and Cursor Up keys to highlight an alarm priority in the console's Alarm Log you want to produce an alarm.
6. With the highlight on the priority you want, press the Spacebar.

   Result: The x changes to a ✓.
7. Repeat the steps for each alarm priority you want included.

Printing

From the Server Printing menu of the Options menu, you can choose one of three destinations for print output from Sniffer servers. You can also specify which server to accept print data from.

If you choose LPT1 or COM1 as your destination, the printer attached to the port should be fast enough to keep up with the output being sent by the server or else the data sent by the server may be lost. If this is a problem, direct the print output first to a disk file, then copy it to the printer later.

Before a server will redirect output to the console, you must configure it to do so. To reconfigure a server to send print data to the console, see "Configuring the Sniffer Server" on page 3–13.

To specify the destination for print output:

1. Use the Cursor key to highlight the **Options** item in the Main Menu.
2. Press the Cursor Right key to move the highlight to the Options menu.
3. Press the Cursor Down key to highlight **Server printing**.
4. Press the Cursor Right key to move the highlight to the Server Printing menu (Figure 4–43).

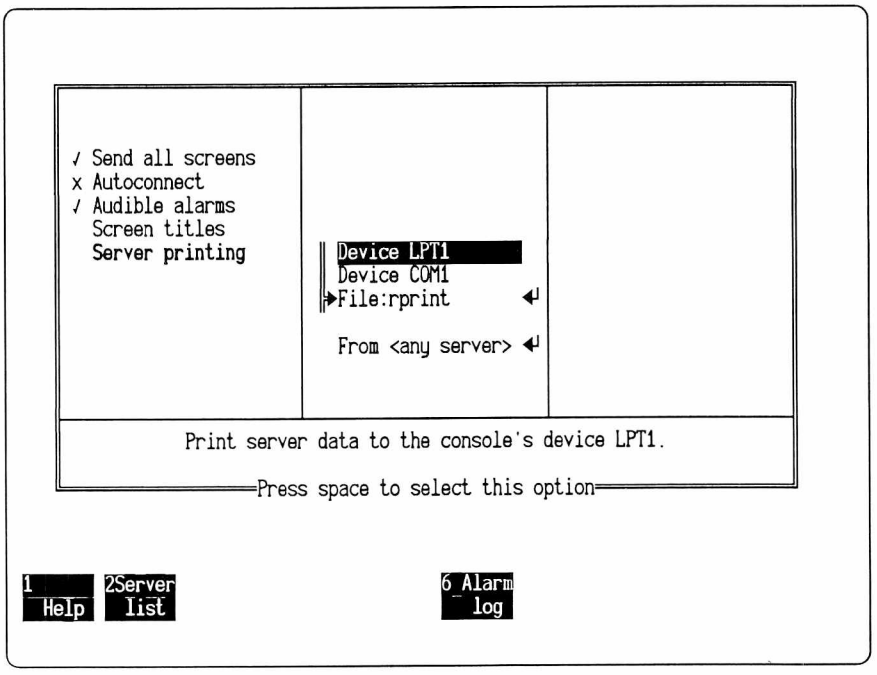


Figure 4–43. Server Printing menu.

5. Use the Cursor Up and the Cursor Down keys to highlight the destination of your choice.
   - **Device LPT1**: SniffMaster console's parallel printer port.
   - **Device COM1**: SniffMaster console's serial port.
   - **File**: File written to the console.
     a. When you highlight this option, press Enter.

        Result: the Enter Pathname dialog box opens so you can specify a pathname (Figure 4–44).
6. Press the Spacebar.

   Result: The pointer moves to indicate your choice.

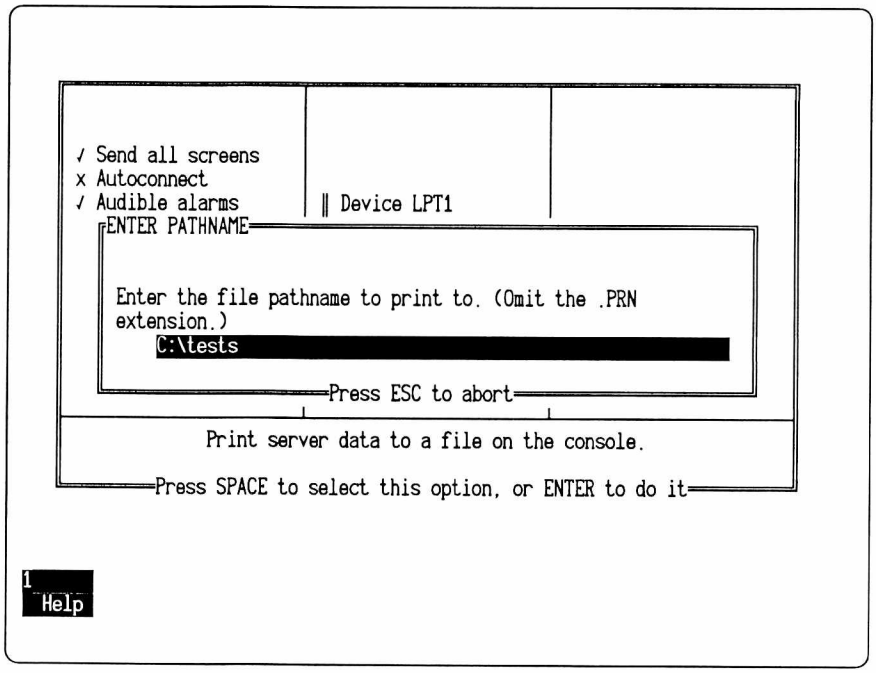


Figure 4–44. Enter Pathname dialog box.

To choose a server from which to receive print data:

1. Use the Cursor keys to move the highlight to the Options\Server Printing menu.
2. Press the Down Cursor to move the highlight to the **From <any server>** item.
3. Press Enter.
4. Look for the Choose Server selection box (Figure 4–45).

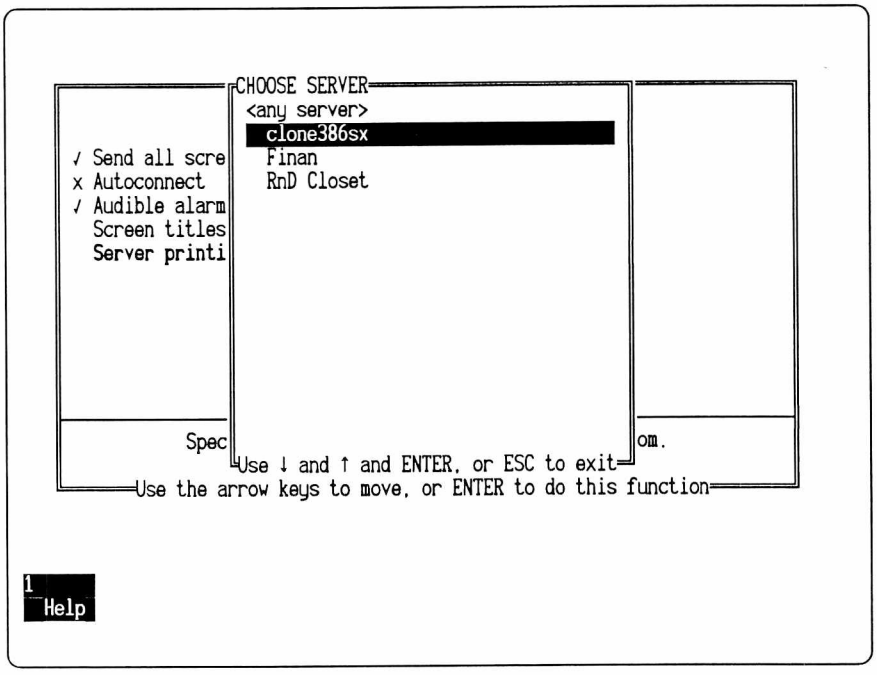


Figure 4–45. Choose Server selection box for server printing.

5. Use the Cursor Up or the Cursor Down keys to highlight the server of your choice.
6. Press Enter to select.

CHAPTER FIVE: SNMP NETWORK MANAGEMENT STATIONS 5

Network General

Chapter 5. SNMP Network Management Stations in the System

Chapter Overview

Alarm information that TCP/IP Sniffer servers send to a SniffMaster console can also be sent to, and displayed on, an SNMP Network Management Station. This chapter explains how you can incorporate SNMP Network Management Stations into your Distributed Sniffer System.

You can also use SNMP GET queries to retrieve Sniffer server trap values. However, this technique is not as efficient as the technique described in this chapter.

Using SNMP Messages

To make use of the SNMP messages, you must first configure your Sniffer servers with TCP/IP to send SNMP messages to target Network Management Stations. For instructions on configuring your TCP/IP Sniffer servers, see "Sniffer Server" on page 3–29.

A Sniffer server sends alarm information to a Network Management Station in SNMP messages. For each user-defined alarm, a Sniffer server sends an SNMP trap. Each trap contains eight NGC variables.

To help you understand management information data bases (MIB) sent by a Sniffer server to a Network Management Station, let's walk through the MIB variables. A typical NGC MIB variable consists of 14 object identifiers written in Abstract Syntax Notation (ASN.1). The first 7 object identifiers are publicly known and identify the ultimate creator of the MIB; the second 7 object identifiers convey alarm information (Figure 5–1).

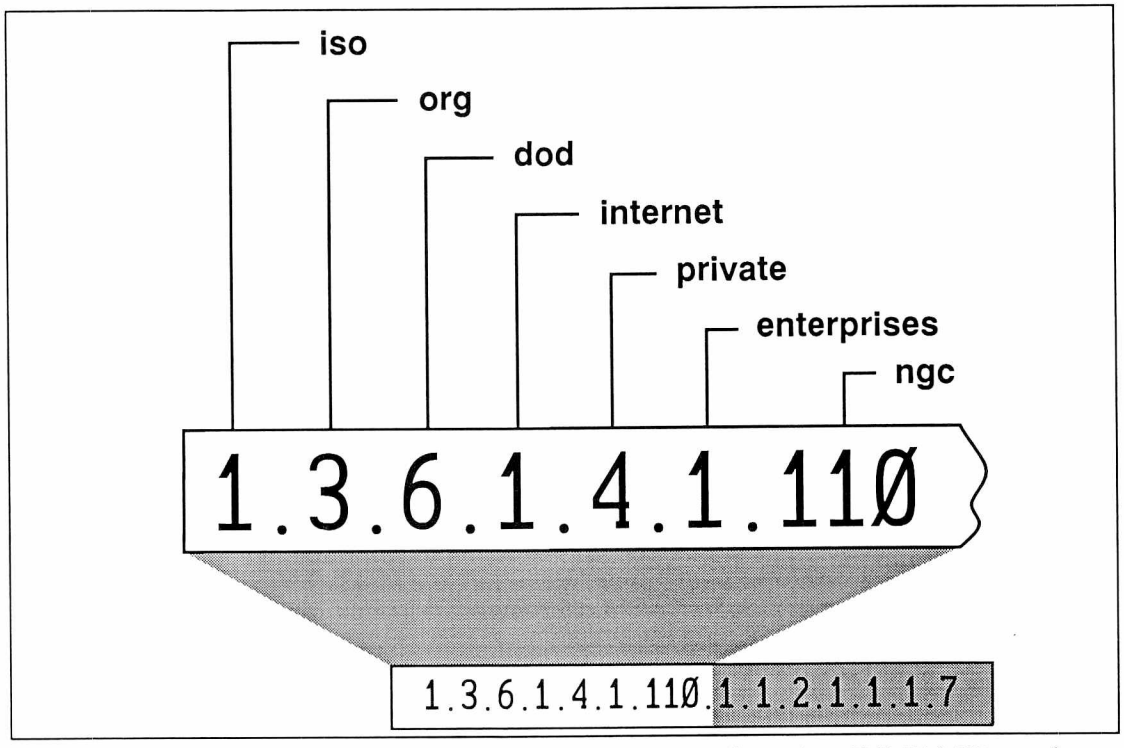


Figure 5–1. Publicly known object identifiers of an SNMP MIB sent by a Sniffer server.

Well-known identifiers occupy the first six variable fields. The identifier in the seventh variable field (**110** or **ngc**) distinguishes each MIB specifically as a MIB administered by Network General Corporation. These first seven identifiers are the same for all traps sent by a Sniffer server to a Network Management Station.

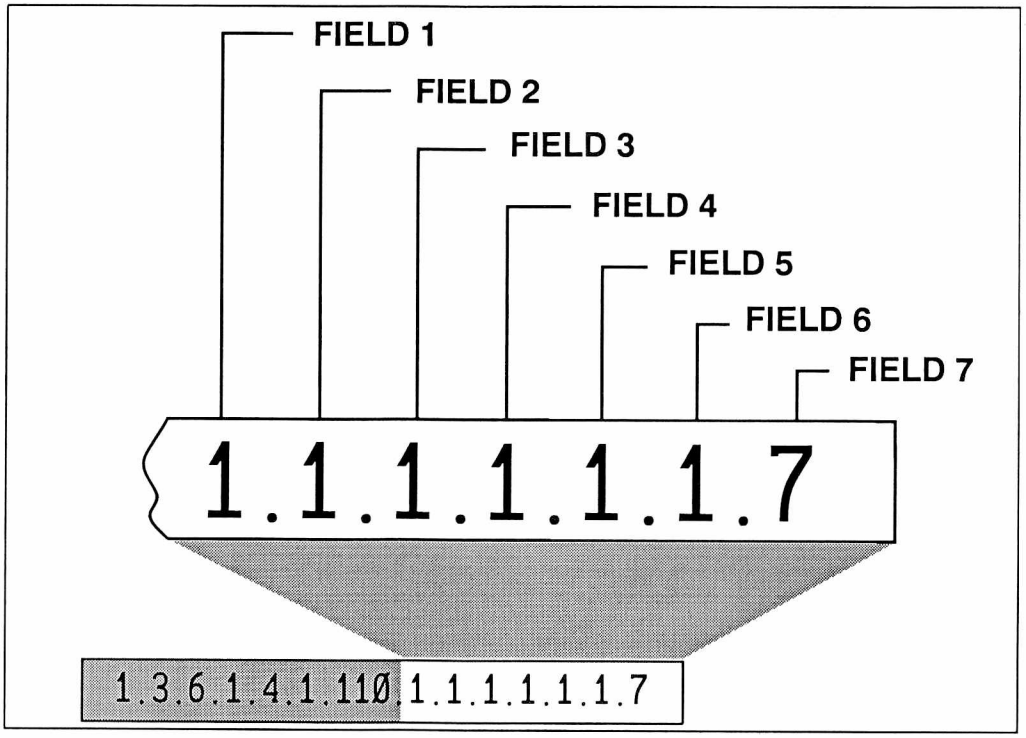


Figure 5–2. Seven fields of alarm information included in an SNMP MIB sent by a Sniffer server.

The second set of seven identifiers specifies NGC MIB version 1 alarm information. Figure 5–2 shows the seven ID fields and gives an example of alarm information. Figure 5–3 shows the seven fields in the alarm information part of an SNMP trap sent by a Sniffer server, the various values that could occupy each field, and the meaning of the value.

According to the information in the table in Figure 5–3, we can tell that a Sniffer server sent this SNMP trap (from the 1 in field 3). In addition, it tells you the timestamp of the alarm (from the 7 in field 7).

Field	Value	Name
1	1	systems
2	1	servers
3	1	Sniffer server
4	1	traps
5	1	traps table
6	1	traps entry
7	1	sequence
	2	ID
	3	text
	4	priority
	5	class
	6	type
	7	time
	8	suspect

Figure 5–3. Fields, values, and names used the alarm information portion of an SNMP MIB sent by a Sniffer server.

The set of seven different object identifiers is basically the same as that sent to, and displayed on, the central SniffMaster console. The full meaning of each part is as follows:

sequence — A counter for keeping track of the order in which each alarm information set is sent.

ID — An integer representing the card number of the board that detected the network event which, in turn, triggered the alarm.

text — The description of the type of network event setting off the alarm.

priority — The level of importance of the network event triggering the alarm. The levels are *inform, warning, minor, major,* and *critical.* For additional information on priority levels, see "Alarm Log" on page 4–46.

class — Indicator of whether the alarm information is for *transmitted frames, received frames,* or *both.*

time — The time the event triggered the alarm.

suspect — The name of the station on the network that triggered the alarm.

APPENDIX A: TROUBLESHOOTING GUIDE A

Network General

Appendix A. Troubleshooting Guide

This appendix lists some common problems you may have with the Distributed Sniffer System and some possible remedies. Hopefully, they will save you some time, some worry, or the need to call for help.

When you suspect a problem with the Distributed Sniffer System, please look through this guide before contacting NGC. Many times we find that correcting a simple oversight can save you (and us) lots of time.

But if our suggestions in this chapter do not solve your problem, please call. Support hours are 6 am to 6 pm Pacific time, weekdays.

Before you call, be prepared to make the following information immediately available when the technical support person comes on the line:

- Locate the Distributed Sniffer System Group Number for the equipment for which you want support. Every piece of Distributed Sniffer System equipment has a Group Number. You will find the Group Number on a label on the bottom of each unit. Record it in the box below.
- Locate the turnkey console and server serial numbers. You will find the numbers on a label on the bottom of each unit.
- Fill out configuration records for consoles and servers and have them available.
- Draw an accurate, up-to-date map of your network that includes LANs as well as interconnecting devices.
- Record any error messages exactly, word for word.
- Provide an accurate description of all symptoms of any problem and, if possible, a description of how to replicate the problem.
- Provide information and analysis from a trace file, if appropriate. If you suspect that the problem is isolated to just a server, to just a console, or to the communications between server and console, you can set a filter on a portable Sniffer analyzer to get a trace that may help.

Distributed Sniffer System Group Number:	
Phone for Network General's Technical Support Department:	(800) 395-3151
FAX:	(415) 321–0855

Some General Troubleshooting Tips

There are a few general approaches to Distributed Sniffer System troubleshooting and common problems you should be aware of as well as simple things you might try for a variety of situations. This section describes some of these.

Problem isolation. Because of the systemic nature of the Distributed Sniffer System, you must try to isolate problems before you can deal effectively with them. Sometimes a problem will be just with a Sniffer server. Other times, a LAN problem that a server is observing is the cause. An interconnecting device can also be a source of problems as can the SniffMaster console itself.

Removing the null modem cable. One problem that seems to come up frequently occurs after the server TCP/IP configuration procedure. A null modem cable is sometimes used as part of the procedure. Users sometimes disconnect the null modem cable from the console but fail to disconnect the other end from the server. When they start to use the server, it does not behave properly. The reason why is that the null modem cable acts like an antenna and picks up signals that interfere with the operation of the server. Make sure the null modem cable is completely detached from both the console and the server.

Rebooting. Sometimes a console will fail to connect to a server or will lose a connection, even though it always seemed to work before. In the sections below, you will find more complex versions of this problem, but there is one solution you should try first. Simply power off the console and power it back on. If that doesn't work, try the same thing on the server. You can reboot a server from the Miscellaneous Controls menu.

Reinstalling and reconfiguring. Sometimes a crucial step in the installation and configuration procedure was inadvertently left out and troubleshooting to find that step is like trying to find the proverbial needle in a haystack. In this case, the most systematic procedure is simply follow the installation and configuration steps from beginning to end to find what was missed.

Recording changes to the distributed Sniffer System and the network. Many times keeping a detailed and accurate history of changes to your network and your Distributed Sniffer System will provide the most important clues for isolating the problem. Among the kinds of changes to pay close attention to are:

- Card configurations
- Software configurations
- NetBIOS addresses
- Subnet masks

- Default gateway addresses
- Reconfigured routers
- Altered bridges
- New router, bridge, or repeater
- New terminate-and-stay-resident (TSR) programs installed that may interfere with the communications software
- Inadvertent changes to CONFIG.SYS and AUTOEXEC.BAT on consoles and servers

Using a portable Sniffer analyzer. A portable Sniffer analyzer is invaluable as a general troubleshooting tool for your Distributed Sniffer System. Below we describe various specific ways that you can use it. It allows you to capture trace files with filters set to capture packets from a console, from a server, or between a console and a server. If you are unable to understand your problem, or to come up with a solution by analyzing the trace file, you can then send the traces to NGC Technical Support for analysis.

Problems on Sniffer Servers

Sniffer servers come with built-in diagnostics. By using them routinely, you can run some quick hardware and software checks.

The sequence of four diagnostic signals following POST (Power-On-Self-Test) tell you how much of CONFIG.SYS and AUTOEXEC.BAT the server has executed. If you do not hear one or more of these signals, you know approximately where the problem occurs by which of the signals you hear and do not hear.

Checking Hardware

This section gives you two procedures for checking hardware. One helps make sure that a server is getting power. The second procedure utilizes POST, a built-in diagnostic, that checks the motherboard, memory, disk drives, and serial ports. A server successfully passes by emitting the first of a sequence of five audible diagnostic signals built into all Sniffer servers. The other four diagnostic signals are used for checking software (see "Checking Software" on page A–7).

To check to see if a server is getting power:

1. Power the server on using the orange power switch in the front of the unit.
2. Look for the green power light in the front of the unit to come on.

- If the light comes on, then you know the server is getting power.
- If the green light fails to come on, you have a power problem.

  a. Check to make sure the power cord is properly attached.

  Note: If the power cord is fine, then additional testing of the power supply is necessary. Try plugging something else into the outlet to see if it works.

To check to see if the server passes the POST (Power-On-Self-Test) for hardware components:

1. Power on the server using the orange power switch in the front of the unit.
2. Listen for a distinct "beep." POST can take over a minute.
   - If you hear the beep, the server passed POST.
   - If you didn't hear the beep, the server did not pass the test. Additional testing on the hardware is necessary.

     Note: POST checks the motherboard, memory, disk drives, and COM port.

     a. Check the hard disk input/output by rebooting and seeing if the fixed disk lamp on the front of the unit flickers. If it does, the hard disk and its controller are probably not the problem.

     b. Check the keyboard terminator. It should be snug and fit properly. You could also take it off and make sure it was not damaged in shipping. It can appear to be ok from the outside.

     c. Check to make sure that the SIMM (Single In-line Memory Module) chips are properly seated. They are located on the motherboard just below the NICs the (Transport Card and the Monitor Card). They should be sticking straight up from the motherboard at 90° angle. There are four in an analysis server; a monitor server has none. Wiggle each one. Push straight down. Make sure you have four of these.

     d. Check to make certain that both NICs are properly seated and parallel to the bus board.

     e. Check that none of the NIC chips (ASICS) have come loose.

Checking Software

Following the hardware check utilizing POST, there are four more diagnostic signals in the sequence emitted following booting of a Sniffer server. These signals tell you how much of CONFIG.SYS and AUTOEXEC.BAT the server has executed. If you do not hear one or more of these signals, you know approximately where the problem occurs by which of the signals you hear and do not hear.

If a server has worked fine for a while and then no longer works as before, a real possibility is that someone has changed the CONFIG.SYS and/or AUTOEXEC.BAT files.

NGC recommends against altering these files in any way. If they have been changed and the server no longer works properly, you may need to reinstall copies of the originals. Hopefully, you made backup copies of these when you first installed your system (see "Backup and Restore Procedures" on page 2–13).

To check that the server's CONFIG.SYS and AUTOEXEC.BAT files execute properly:

1. Reboot the server.
2. Make certain that the server passes POST.
3. Listen for the sequence of four more diagnostic signals that indicate the stages of execution of CONFIG.SYS and AUTOEXEC.BAT:

Checkpoint 1 One tone indicating that the operating system environment has been set.

Note: *Checkpoint 1* may be especially important if you are configuring TCP/IP on a server and have attached a terminal, or a PC running terminal emulation software, with a null modem cable. *Checkpoint 1* tells you that IOFORK.SYS, a TSR utility, has been installed. This TSR sets up the COM1 serial port so the server can accept keyboard input and can send out diagnostic messages to a terminal or PC screen.

Checkpoint 2 Two tones indicating that memory has been initialized.

Note: Failure to pass *Checkpoint 2* may indicate that the SIMM chips are improperly seated. They are located on the motherboard just below the NICs the Transport Card and the Monitor Card). They should be sticking straight up from the motherboard at 90° angle. There are four in an analysis server; a monitor server has none. Wiggle each one. Push straight down. Make sure you have four of these.

Checkpoint 3 Three tones indicating that the communications software has been installed.

Note: TCP/IP requires nothing to be attached to the server to initialize its Transport Card. Two transport protocol drivers—NetBEUI for token ring and IPX for both token ring or Ethernet—will hang if the Transport Card is not connected to something (either to a network or to a loopback hood):

- If you have NetBEUI, just attach a token ring cable to the server's 9-pin connector. The cable is self-shorting so it acts like a loopback hood.
- If you have IPX for "thin" Ethernet, use a BNC-T connector with a 50 ohm terminator on each side of the "T" as a loopback hood.
- If you have IPX for "thick" Ethernet, attach the AUI cable into a transceiver and then terminate the transceiver with a loopback hood.
- If you have IPX for token ring, just attach a token ring cable to the server's 9-pin connector. The cable is self-shorting so it acts like a loopback hood.

Musical Chime Indicating that the server is ready.

Note: It is possible for a server to emit the *Musical Chime* and still not run properly. You may not notice anything until you try to connect to the server with a console. If you used a null modem cable to configure TCP/IP on a server, make sure the null modem cable is no longer attached. If it is left attached, it acts like an antenna and picks up signals that may disrupt the server.

Problems on SniffMaster Consoles

There are two basic types of SniffMaster console. The *turnkey* console is relatively trouble-free. If there are any problems, the most likely source would be manufacturing or shipment damage. There are a few other things to look out for. The *board-and-software* console, however, could have some of the problems of the turnkey version, so look those over. Or it could have been installed incorrectly.

Turnkey Version

The turnkey version of the SniffMaster console comes preconfigured to your specifications. It should work right out of the box. There are a few hardware and software problems for which you might want to look.

Checking Hardware

There are three hardware problems you can check out quickly and routinely. This section describes the procedure for checking two of the three problems.

The third possible problem was described earlier and applies only if you used the console to configure TCP/IP on a server. If you do this, always make sure you remove the null modem cable from both the server and the console. Neither will work properly if the cable is left connected.

To determine if a console is getting power and if the hard disk is accessible:

1. Power on the console.
2. Look for the green power light in the front of the unit to come on.
   - If the light comes on, then you know the console is getting power.
   - If the green light fails to come on, you have a power problem:
     a. Check to make sure the power cord is properly attached.

        Note: If the power cord is fine, then additional testing on the power supply is necessary. Try plugging something else into the outlet and see if it works.
3. Look for the hard disk input/output lamp to flicker:
   - If the light flickers, then you know that the hard disk and its controller are probably working properly.
   - If the light fails to come on and flicker, then additional testing on the power supply is necessary. Try plugging something else into the outlet and see if it works.

Checking Software

You may have a problem at a console that prevents it from establishing connections to servers: sometimes transport protocol drivers will not boot or fail to initialize the Transport Card.

TCP/IP will initialize the Transport Card regardless of whether the card is attached to anything or not. Two transport protocol drivers—NetBEUI for token ring and IPX for both token ring or Ethernet—will hang if the Transport Card is not connected to something (either to a network or to a loopback hood):

- If you have NetBEUI, just attach a cable to the console's 9-pin connector. The cable is self-shorting so it acts like a loopback hood.
- If you have IPX for "thin" Ethernet, use a BNC-T connector with a 50 ohm terminator on each side of the "T" as a loopback hood.
- If you have IPX for "thick" Ethernet, attach the AUI cable into a transceiver and then terminate the transceiver with a loopback hood.
- If you have IPX for token ring, just attach a cable to the console's 9-pin connector. The cable is self-shorting so it acts like a loopback hood.

Board-and-Software Version

The board-and-software version of the SniffMaster console could possibly have any of the hardware or software problems described for the turnkey version. Because of the additional steps required for installation and configuration, or because of the use of hardware for which the console was not specifically designed, the board-and-software version could have other kinds of problems.

The most likely problem will be the Transport Card configuration. NGC recommends that the PC you choose be dedicated as a Distributed Sniffer System console. It is quite possible that you will choose a PC that was used for something else before and has other cards in it already. It is also possible that you intend to keep some or all of those cards in the machine and to keep using it for some or all of its previous uses. (NGC recommends against this.) Finally, given this situation, it is quite possible that there are configuration conflicts between the Transport Card shipped to you by NGC and the cards already installed in the console candidate PC.

In the latter case, various types of problems will be traceable to conflicts in board settings. To help your record-keeping and troubleshooting, we provide (see Figure A–1 and Figure A–2) the jumper and switch settings for the two types of console Transport Card—the InterLan NI5210 and IBM 16/4 Token Ring—as preset at the factory. We recommend that you also record along with this all card settings for cards already in the PC.

Parameter	Jumper	Setting
I/O Base Address=310H	8	B
	7	A
	6	A
	5	A
	4	B
	3	A
Memory Base Address=d000H	17	A
	16	B
	15	A
	14	A
Extended Memory Socket	XME	B
	XRE	B
IBM PC XT Slot Selection=OFF	W27	OFF
Interrupt Request (IRQ) Level=3	IRQ	3
Legend: A=jumper setting A B=jumper setting B OFF=jumper disabled		

Figure A–1. Factory jumper settings for the NI5210 Ethernet Transport Card of board-and-software console.

If you are using TCP/IP as your transport protocol, you have several additional steps after checking the jumpers on the card. You also need to check the software that recognizes the hardware

To check the command line parameters for the InterLan card driver when using the TCP/IP transport protocol.

1. If necessary, exit to the DOS prompt from the console application.
2. Change to the directory containing the file, NGCEXEC.BAT. If you installed the console software to the default installation directories, type

   C:\CD CONSOLE\WINTCP

3. Using the DOS line editor, EDLIN, or some other text editor, check the command line that installs the driver for the InterLan card.The line should look like this:

```
interl -I:3 -B:310 -M:D000
```

-I: Interrupt Request Level

-B: I/O Base Address

-M: Memory Base Address

Parameter	Switch	Setting
ROM Address=dc00H	1	U
	2	D
	3	U
	4	U
	5	U
	6	D
Interrupt Level=3	7	D
	8	D
Primary/Alternate=primary	9	U
Shared RAM Size=16KB	10	U
	11	D
Adapter Data Rate=16/4Mbps	12	U=16 D=4
Legend: U=switch is up D=switch is down		

Figure A–2. Factory switch settings for the token ring 16/4 Transport Card of board-and-software console.

Console-Server Connection Problems

There are numerous problems that may occur with console-server connections. In this section, we describe several possible reasons why consoles do not connect with servers. Some of these apply to the situation where you try to connect for the first time. Others apply to situations where a connection that worked before stops working. Some of these problems depend on which transport protocol you use.

Server Address Problems

One reason you may not make a connection is that there is an incorrect NetBIOS or TCP/IP address. In this section, we describe several ways in which the wrong address may have been used.

NetBIOS Address Incorrectly Derived

The NetBIOS address is preconfigured at the factory. You must derive it from the board address of the Transport Card. To do this, you will need to check the board address on the label underneath the server, use it derive the NetBIOS address, and then check that against the NetBIOS address as recorded in the console's server database.

To compare the NetBIOS address of a server against the NetBIOS address recorded on a console's server database:

1. Find the board address label attached to the bottom of the server.

   Note: The board address has 12 hex characters, for example, 10005A786E82 (hex). You will use the last 6 characters of this board address to derive the NetBIOS address assigned at the factory.

2. To derive the NetBIOS address, delete the first 6 characters of the board address:

   - **Token ring.** If you have a token ring board, substitute NGCT for the first 6 characters of the address. Using the address above as an example, you would have a NetBIOS address of NGCT786E82.
   - **Ethernet.** If you have an Ethernet board, substitute NGCE for the first 6 characters of the address. For example, a board with the address, 02070108159c, would have the NetBIOS address, NGCE08159c.

3. On the console's Main Menu, use the cursor keys to highlight the **Manage name** item.
4. Press the Enter key.
5. Compare the NetBIOS address recorded there with the address you derived from the server's board address. They should be the same.

Confusing Default NetBIOS Address, User-Defined NetBIOS Address, and Symbolic Name

Another potential problem is confusion among three types of reference to a server:

- *Default NetBIOS address* preconfigured for each server at the factory. You derive the NetBIOS address from the Transport Card address during the installation procedure. This address is entered into a console's server database through the NetBIOS address field of the Manage Names dialog box. The address will appear in the Transport Address column of the Server Status display.

- *User-defined NetBIOS address* defined by the user in the Server Configurator. This address serves exactly the same function as the default NetBIOS address and supersedes the NetBIOS address preconfigured for the server at the factory. You would choose to use a user-defined NetBIOS address if you wanted to make a server more readily identifiable, e.g., to distinguish among groups of servers or specialized functions of particular segments or rings. This address is entered into a console's server database through the NetBIOS address field of the Manage Names dialog box. The user-defined NetBIOS address will appear in the Transport Address column of the Server Status display.
- *Symbolic name* defined by the user in the console's server database through the name field of the Manage Names dialog box. This name serves no purpose other than to make a server more identifiable. It will appear in the Server Name column of the Server Status display.

Changing the NetBIOS address and failing to enter it properly on the console's server database can create a very big problem. For example, someone may define a new NetBIOS address on a server from one console and not inform users at another console. Or someone defines a new NetBIOS address but enters it in the name field, instead of the address field, of the Manage Names dialog box.

If you override the default NetBIOS address by creating a user-defined NetBIOS address, you must enter the user-defined address in the NetBIOS address field of the Manage Names dialog box. If you don't, the console won't be able to find the server.

If you have reason to think that this may be the problem, you need to find out what the current user-defined NetBIOS address (if one was created) is on the server and to compare it to the information for that server in the console's server database. Since the console cannot find the server, you need to use a separate utility to extract the information from the server.

To find the user-defined NetBIOS address and to compare it with the server information entered in the server database:

1. Use the server's Transport Card address and the NetBIOS Adapter Status Utility to retrieve server information.

   Note: For instructions on the use of this tool, see "NetBIOS Adapter Status Utility" on page B–7. This utility retrieves information, including the user-defined address if one was created to override the default address, from any NetBIOS station on the network.

2. Find the NetBIOS Name Table in the retrieved information. If there is a new user-defined NetBIOS address, it will appear in

that table.

3. Go to the Server Status display on the console.
4. Compare the user-defined address you found by using the NetBIOS Adapter Status Utility with the Transport Address for that server. Both should be the same.
5. If the two addresses are not the same, enter the address retrieved with the utility into the server's database using the Manage Names display.

Inaccurate IP Address, Subnet Mask, and Default Gateway Information

An obvious source of problems for those who use TCP/IP as their transport protocol is inaccurate IP address, subnet mask, and default gateway settings. To eliminate any problems caused by such errors, you need to compare the current settings on the server to which you cannot connect with the information in the console's server database.

To check the current settings for the server, console, and gateways:

1. Power off the server.
2. Since you cannot connect with the server, you'll need to attach an external device to it. See "To attach a PC or terminal to a Sniffer server:" on page 3–29.
3. Make certain the Transport and the Monitor Cards are connected.
4. Enter terminal emulation mode with the external device. See "To enter terminal emulation mode using the SniffMaster console:" on page 3–30.
5. Power on the server.

   Result: The sequence of server diagnostic tones and messages will sound and appear. Then the Sniffer server IP Initialization Program menu appears.
6. When you see the Sniffer server IP Initialization Program menu, press any key immediately to pause.
7. Check the current settings for the server. You will see them in the column on the right-hand side of the screen (see Figure 3–17):

IP address — Check the address entered against the actual address assigned to this server. Also compare this with the address entered for this server in the console's database.

Subnet mask	Make certain this was entered correctly. You enter the subnet mask in terms of the number of subnet bits. Typically, this would be a number between 8 and 24. 8 creates a subnet mask of 255.0.0.0. 24 creates a subnet mask of 255.255.255.0.
Default gateway	Compare this with the actual address for the default gateway.

8. Make certain the server's Transport Card is connected to the network.
9. Reboot the console.

   Result: The SniffMaster console IP Initialization Program menu appears.
10. When you see the SniffMaster console IP Initialization Program menu, press any key immediately to pause.
11. Check the current settings for the console. You will see them in the column on the right-hand side of the screen (see Figure 3–14):

IP address	Check the address entered against the actual address assigned to this console.
Subnet mask	Make certain this was entered correctly. You enter the subnet mask in terms of the number of subnet bits. Typically, this would be a number between 8 and 24. 8 creates a subnet mask of 255.0.0.0. 24 creates a subnet mask of 255.255.255.0.
Default gateway	Compare this with the actual address for the default gateway.

Too Many Consoles Trying to Connect to the Same Server

Servers can be configured to connect to up to two consoles. If a server is configured to one console, then all others trying to connect will be rejected. The same is true for a server configured to two console connections.

Sometimes you may lose a connection to a server and, before you can reestablish the connection, another console may have connected already, and the server reaches the maximum for which it was configured.

Another situation is where someone may have changed a server's configuration without properly notifying personnel working at other consoles. It is possible that where a server was originally configured to accept up to two consoles, it was reconfigured to accept only one.

When you try to connect, you can no longer do so because of the change in the server.

The clues that indicate that this is the case vary, depending upon the transport protocol you use:

- If you have TCP/IP, you will see the message, "Server connection rejected," when a server has its maximum number of connections. The message tells you that the server is alive and well but that it cannot accommodate any more consoles.
- If you have NetBIOS, you will see a message with the name of the server already connected when the server is configured for one console connection. When configured for two console connections, the server will tell you only that the connection attempt failed.

What you'll need to do is to first check to see how many console connections for which the server is configured. Then you'll need to check that against how many consoles can potentially connect to that server.

To compare a server's console connection configuration with the number of consoles that could potentially connect to that server:

1. Find a console with an established a connection to the server.
2. If an application is running on the server, go to the Main Menu, and use the Cursor keys to highlight the Exit item.
3. Press the Enter key.

   Result: The Main Selection Menu appears.

   Note: If you are running the monitor application, the monitor may still be running in background. If that is the case, you will need to shut it down:

   a. Highlight the monitor application item in the Main Selection Menu.

   b. Press the Enter key.

      Result: The Monitor Services Menu appears.

   c. Highlight the **Shutdown the Background Processes** item.

   d. Press the Enter key.

      Result: You will be prompted to confirm shutting down background processes and then returned to the Main Selection Menu.

4. In the Main Selection Menu, highlight the **Configure Server** item.

5. Press the Enter key.

   Result: If you have an analysis application on the server, the Configure Analysis Server menu appears.

   a. With the highlight on **Server Parameters**, press Enter.

      Result: The Server Configurator Main Menu appears.

6. Check the **Consoles=** item in the Main Menu of the Server Configurator. The server could be configured for either one or two consoles.

7. Check the server databases of each console that could potentially connect to the server:

   a. Go to the console's Main Menu.

   b. Use the Cursor keys to highlight the **Manage names** item.

   c. Press the Enter key.

   d. Check to see if the server's address is listed.

   e. Repeat these steps for each of the other console's.

8. Compare the number of consoles with the server's address in their server database with the number of console connections for which the server is configured.

   Note: If the number of consoles that can potentially connect to a given server exceeds the number of console connections for which it is configured, then you run the risk of console rejection. You will need either to change the configuration on the server or find some way to manage the connection of consoles to servers.

Problems With Interconnection Devices

It's important to know the interconnection devices—e.g., a bridge or a router—between a console and a server. These can be turned off, or they can be configured to filter certain types of packets. In this case, you may want to put a portable Sniffer analyzer on either side of the interconnection device to see if server packets or console packets are getting through. For example, consoles and servers in the TCP/IP environment require ARP (Address Recognition Protocol) requests and replies in order to establish a connection. If the interconnection device is set to filter on ARP packets, a connection will never be established.

Duplicate IP Addresses

If you get the message, "Transfer connection rejected," it could indicate duplicate IP addresses, Use the following procedure:

To check for duplicate IP addresses:

1. Power off the console.

   Result: This will clear the ARP cache. If it was cached in memory, it will not do another ARP.

2. Set up a portable Sniffer analyzer to capture frames sent out of the console's transport card and packets received by the card.
3. Power the console back on.
4. Go to the Server Status window of the console.
5. Try to connect to any server in the list.
6. Look for any ARP request from the console on the Sniffer analyzer.
7. When you see the ARP Request, look for the IP address of the server you are trying to connect to. Make sure it matches the address to which you are trying to get.
8. On the portable Sniffer analyzer, look for the ARP Reply.

   Result: If you get an ARP Reply from any device other than the server to which the original ARP Request was intended, then you have a duplicate IP address.

APPENDIX B: TROUBLESHOOTING AND FINE TUNING UTILITIES B

Appendix B. Troubleshooting and Fine Tuning Tools and Utilities

This appendix explains several tools and utilities for troubleshooting and fine tuning your Distributed Sniffer System. There are four of these covered:

- Two additional commands on the IP Initialization Program Menu
- PING utility
- NetBIOS Adapter Status utility
- IOFORK.SYS device driver.

Expanded TCP/IP Initialization Program Menu

"Configuring TCP/IP" on page 3–26 explains how to use the Initialization Program to configure TCP/IP on both servers and consoles. Two additional commands let you set additional configuration options for the TCP/IP stack. Both are on a special "hidden" version of the program's menu. The two commands are summarized in Figure B–1.

Command	Function
connections	Sets the number of connections to the unit. For a *server*, the range is 1 to 2 console connections. For a *console*, the range is 1 to 32 server connections.
window	Sets the size of the TCP window. Select a multiplier from 1 to 8. The multiplicand is the "maximum segment size."

Figure B–1. Expanded Initialization Program Menu options.

When using the **connections** command with a console to connect servers, remember that 30 connections is an upper limit tested by NGC on some network configurations. Optimal performance of the Distributed Sniffer System will be less on other network configurations.

You will use the **window** command when adjusting the stack for a "slow" versus a "fast" network. Use higher multipliers for slower networks to insure that all data is received. A large multiplier sets a large buffer for the TCP window mechanism, and that, in turn, uses up valuable memory. Therefore, if your network is fast enough to handle the data, decrease the size of the window.

The TCP window mechanism is a flow control tool. It works with the acknowledge mechanism to update senders and receivers as data is

transmitted and received. A receiver periodically empties its buffer, acknowledges received data, and tells the sender its current window size, i.e., the size of the buffer it has available for additional data. The sender then subtracts the amount of data already sent from that window size and uses the difference to determine how much more data it can send.

To open the expanded IP Initialization Program Menu:

1. Exit to the DOS command line. Are you opening the IP Initialization Program on the console or a server?

- If you are using the console.

  a. Use the Cursor keys to highlight **Exit** in the Main Menu.

  b. Press Enter.

  Result: The DOS command line appears.

- If you are viewing a monitor or analyzer application on the console display:

  a. Use the Cursor keys to highlight **Exit** in the Main Menu.

  b. Press Enter.

  Result: The Main Selection Menu appears.

  c. Use the Cursor key to highlight **Exit to the Operating System** or, alternatively, Escape.

  d. Press Enter.

  Result: The DOS command line appears.

2. At the DOS prompt, type IPINIT -f.
3. Press Enter.

   Result: The expanded IP Initialization Program Menu appears (Figure B–2).

```
Network General IP initialization program.  Version Ø.Ø7
(C) Copyright 1991, Network General Corporation
Using wintcp info file C:\CONSOLE\wintcp\wintcp.sys

If you change any settings, this system will optionally reboot when you quit.

        Ipinit commands (and current settings) :
address    - Set IP address             [currently set to Ø.Ø.Ø.Ø]
connections - Set number of connections  [currently set to 32]
subnet     - Set IP subnet mask          [currently set to Ø.Ø.Ø.Ø]
gateway    - Set default IP Gateway      [currently set to Ø.Ø.Ø.Ø]
targets    - Set SNMP trap targets       [currently set to none]
window     - Set TCP window multiple(#*mss)  [currently set to 3]
help       - Display this menu
quit       - Exit to DOS
update     - Save changes

Hit any key (within 5 seconds) if you want to change anything:
Ipinit>
```

Figure B–2. Expanded TCP/IP Initialization Program Menu.

4. Type the appropriate Ipinit command for the setting you want to change (i.e., **connections** or **window**).
5. Press Enter.
6. Follow the instructions that appear to change the setting.
7. When finished, type **update** or "**u**."
8. Press Enter.
9. Type **quit** or "**q**."
10. Press Enter.

    Result: The DOS prompt reappears. You will be prompted as to whether or not you want to reboot. You need to reboot for the changes to take effect. If you do reboot, you'll need to reconnect.

11. If you didn't reboot, you can return to the Main Selection Menu by typing MENU at the DOS prompt.
12. Press Enter.

    Result: The Main Selection Menu reappears.

PING Utility

You can use a tool called PING for TCP/IP Distributed Sniffer System testing and management. PING is an echo request program that uses the Internet Control Message Protocol (ICMP). Its primary use is to determine the operating status of specific IP addresses on the system.

One typical scenario for using PING is when you want to check to make sure that you are getting traffic out from the console through a router to a server and then getting a reply back. What you can do is to first try a workstation on the console side of the router. Next try the card of the router itself. Then send a PING through the router to workstations on the other side of the router.

Another scenario is asymmetrical where you can PING successfully one way but replies do not get back through. For examples, routers could have been set up to filter on an IP address one way but not the other. In this case, you can have someone at the other end PING back to you. Again, use the strategy described above: PING locally, then to the interconnection device, and then through the interconnection device.

To use PING to check IP address status:

1. Exit to the console's DOS command line:

   a. Use the Cursor keys to highlight **Exit** in the Main Menu.

   b. Press Enter.

   Result: The DOS command line appears.

2. At the DOS prompt, type

   PING *IPaddress* [-s] [-z] [-n] [-t] [-o] [-i]

   For example,

   PING 89.0.0.56

   Note: There are a variety of command-line options available:

Option	Option Name	Function
-s		Sends request datagrams to a server continuously until you press a key. If the datagrams do not stop, type "q" to quit.
-z	datasize	Specifies the number of bytes sent in each request datagram. Maximum is 512 bytes. Default is 64 bytes.
-n	packets	Specifies how many request datagrams to send.
-t	time	Specifies in seconds the length of time to send datagrams. Console will send as many as possible, given the value for -i interval.
-o	timeout	Specifies in seconds the length of time for the console to wait for a response datagram. Default is 5 second.
-i	interval	Specifies in seconds the length of the interval between each transmitted request datagram. Default is 1 second.

Figure B–3. Command-line options for the PING utility.

3. Press Enter.

   Result: A message appears on the screen indicating that the unit with the IP address is operating.

4. To return to the console application, type CONSOLE at the DOS prompt.

5. Press Enter.

   Result: The console's main menu appears.

NetBIOS Adapter Status Utility

You can use the NetBIOS Adapter Status Utility, NBPING, for troubleshooting your Distributed Sniffer System much like PING. It comes already installed with your console software. The main purpose of the utility is to verify the presence of other NetBIOS stations on a network. When you invoke it, you will see a screenful of information about the adapter in the server to which you directed it: its permanent and software-selectable names, statistics, and local name table data.

Figure B–4 shows an example of the adapter status and name table data retrieved by the NetBIOS Adapter Status Utility:

```
NetBios Adapter Status:
   Unit Id (hex)            = 1Ø ØØ 5A 78 72 6D
   Version                  = 1.Ø
   Reporting Period (mins)  = 2327
   Collisions               = Ø
   Aborted Transmits        = 1
   Packets Transmitted      = 6269
   Packets Received         = 6477
   Retransmissions          = 3
   Free NCBs                = 1Ø
   Max. Configured NCBs     = 12
   Max. Total NCBs          = 12
   Pending Sessions         = 2
   Max. Configured Sessions = 32
   Max. Total Sessions      = 32
   Max. Packet Size         = 4Ø96
   NetBios Names in Table   = 1

NetBios Name Table:
   Num:   Type:   Status:   NetBios Name:
   ---    ----    ------    ------------
   ØØ2    Unique  REG       NGC1ØØØ5A78726D.

C:\CONSOLE>
```

Figure B–4. Example of data retrieved by NetBIOS Adapter Status Utility.

As Figure B–4 shows, the data is displayed in two parts: NetBIOS Adapter Status and NetBIOS Name Table. The sections below describe each data category.

NetBIOS Adapter Status Data

Unit ID	A number assigned the adapter during manufacturing. It is the last six bytes of the permanent node name.
Version	Software version number of the NetBIOS release.
Reporting Period	Number of minutes during which adapter statistics have been collected. The counter is reset only by a power-on reset, and it does roll over when it reaches maximum count.
Collisions	Number of collisions detected during datagram transmissions since counter reset or turned over.
Aborted Transmits	Number of datagram transmissions stopped by the adapter since counter reset or turned over.
Packets Transmitted	Number of packets successfully transmitted since counter reset or turned over.

Packets Received	Number of packets successfully received since counter reset or turned over.
Retransmissions	Number of retransmissions of remote adapter status calls that have occurred since counter reset or turned over.
Free NCBs	Number of available Network Control Blocks (NCB) not in use. An NCB is a block of memory containing information about a command passed to NetBIOS.
Max. Configured NCBs	Number of NCBs configured during initial NetBIOS configuration.
Max. Total NCBs	Number of NCBs allowed by last RESET command.
Pending Sessions	Number of sessions currently pending. A "session" is a reliable two-way connection between two names on the network. A server can have up to two sessions (with each of two consoles) at one time.
Max. Configured Sessions	Number of sessions configured during initial NetBIOS configuration. The Distributed Sniffer System allows only two.
Max. Total Sessions	Number of sessions allowed by last RESET command.
Max. Packet Size	Maximum session data packet size.
NetBIOS Names in Table	Number of NetBIOS names currently registered in the local names table.

NetBIOS Name Table

Num	Name number. Used by many NetBIOS commands as a quick way of referring to a name known to be in the local names table.
Type	Type of name. An adapter reserves a "unique" name for its exclusive use on the network. Other adapters can use a "group name."

Status	Current status of the name entry. The statuses are: attempting to register name, name registered, name de-registered, name duplicated, and name duplicated but de-registration pending.
NetBIOS Name	Software-selectable name. This name can be recognized on the network. NGC supplies each adapter with a name at the factory. When a user substitutes another name when configuring a server, the new name takes the place of this name.

To use NBPING to check adapter status:

1. Exit to the console's DOS command line:

   a. Use the Cursor keys to highlight **Exit** in the Main Menu.

   b. Press Enter.

   Result: The DOS command line appears.

2. Change to the directory with NBPING. Are you attached to an Ethernet or a token ring?

   - If Ethernet, type at the DOS prompt

     C:\CD\CONSOLE\IPXEN

   - If token ring, type at the DOS prompt

     C:\CD\CONSOLE\IPXTR

3. At the DOS prompt, type

   NBPING NAME=*NetbiosName* [HEX] [SEC]

   Note: NetBIOS names are case-sensitive. You can use the permanent node name in place of the NetBIOS name, but it requires special notation. You must enclose the hex digits of the permanent node name in brackets:

   [*xxxxxxxxxxxx*]

   The HEX parameter displays the name in hexadecimal. The SEC parameter accesses the secondary adapter.

4. Press Enter.

   Result: NBPING returns the statistics display (Figure B–4).

5. To return to the console application, type CONSOLE at the DOS prompt.

6. Press Enter.

   Result: The console's main menu appears.

IOFORK.SYS Utility

The IOFORK.SYS utility is specified in the CONFIG.SYS file and is used when configuring TCP/IP servers from a serial device at their local serial port (see "Sniffer Server" on page 3–29) and for troubleshooting on all servers. You probably will never have to adjust IOFORK.SYS, but if you do, we provide a description of how you can do that.

You can create serious problems when inappropriate changes are made that conflict with other portions of the server.

The command line in CONFIG.SYS would look like this:

```
DEVICE=\TOOLS\IOFORK COM#:Speed,Parity,Databits,Stopbits
```

#	COM port number. Use 1 or 2.
Speed	Baud rate. Enter only the first two digits of the speed. Speeds support are 300, 1200, 2400, 4800, 9600, and 19.2K.
Parity	Parity may be O, E, and N for "odd," "even," or "no parity."
Databits	Databits may be 5 to 8.
Stopbits	Stopbits may be 1 or 2.

An example would be:

```
DEVICE=IOFORK COM2:48,O,7,2
```

The example sets IOFORK.SYS to use COM port 2, baud rate 4800, odd parity, 7 data bits, and 2 stop bits.

The COM port and speed are required on the command line; however, the other trailing parameters may be changed or omitted. NGC sets the parameters at 9600 baud rate, no parity, 8 data bits, and 1 stop bit in CONFIG.SYS.

You can use COM ports other than 1 or 2. IOFORK.SYS allows the interrupt vector and IO base for its COM1 UART (Universal Asynchronous Receiver Transmitter) table to be overwritten from the command line. The commands for setting these are IRQ:*x* and BASE:*xxxx*. The interrupts can be 0 to 7; the IO base can be 200 to FFFF (hex). An example would be:

```
DEVICE=\TOOLS\IOFORK.SYS IRQ:5 BASE:02F8 COM1:96
```

The example configures IOFORK.SYS to use a UART at interrupt vector 5 and IO base 02F8 (hex).

APPENDIX C: CONFIGURATION RECORD C

Network General

Appendix C. System Configuration Record

Starting a System Configuration Record

Like your network itself, your Distributed Sniffer System needs to be well-documented for both the maintenance of the system as well as to track the changes you will inevitably make to it.

You may already have a network documentation system that works well for you. In that case, you may find the suggestions contained herein helpful in developing any modification to your current system made necessary by installing a Distributed Sniffer System.

If you want a separate record-keeping system specifically geared for the Distributed Sniffer System, then you may want to adopt the configuration forms contained in this appendix.

The "Console Configuration Form" on page C–4 and "Server Configuration Form" on page C–5 are two sample forms you can use to document console and server configurations. The fields on the forms represent the most important configuration information based on NGC's experience with the Distributed Sniffer System products.

We also recommend that you maintain an up-to-date map of your system. Be sure to note:

- Specific servers observing the different segments, rings, and links
- Consoles controlling specific servers
- Interconnection devices and their addresses.

Console Configuration Form

Address/Alias

IP/NetBIOS Address _____ Alias _____

Sniffer Servers Controlled by this Console

	IP/NetBIOS Address	Alias
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

Transport Protocol

☐ NetBIOS/NetBEUI
Configuration Parameters _____

☐ NetBIOS/IPX
Configuration Parameters _____

☐ TCP/IP

		Defaults
IP	_____	0.0.0.0
Subnet Mask	_____	24 bits (255.255.255.0)
Default Gateway	_____	0.0.0.0

Console Hardware

Board-and-Software Configuration

PC Vendor _____
RAM _____
Hard Disk _____
Monitor _____
ISA Slot _____
EISA Slot _____

Driver

IRQ _____
I/O Address _____
Buffer _____
DMA _____

Transport Card

Token ring ☐ 4 Mbps ☐ 16Mbps

Ethernet ☐ Thick ☐ Thin

Server Configuration Form

Server Address

IP/NetBIOS Address _____

Consoles Controlling this Server

	IP/NetBIOS address	Alias
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____

Transport Protocol

☐ NetBIOS/NetBEUI
Configuration Parameters _____
_____
_____

☐ NetBIOS/IPX
Configuration Parameters _____
_____
_____

☐ TCP/IP

		Defaults
IP	_____	0.0.0.0
Subnet Mask	_____	24 bits (255.255.255.0)
Default Gateway	_____	0.0.0.0

SNMP Trap Targets

IP Address	_____	Community Name	_____
IP Address	_____	Community Name	_____
IP Address	_____	Community Name	_____
IP Address	_____	Community Name	_____
IP Address	_____	Community Name	_____
IP Address	_____	Community Name	_____

Network Interface Cards

Transport Card

☐ Token ring ☐ 4 Mbps ☐ 16 Mbps

☐ Ethernet ☐ Thick ☐ Thin

Hardware address _____
Jumper/ switch settings _____
_____
_____

Monitor Card

☐ Token ring ☐ 4 Mbps ☐ 16 Mbps

☐ Ethernet ☐ Thick ☐ Thin

☐ WAN

Hardware address _____
Jumper/ switch settings _____
_____
_____

INDEX

Index

D

E

F

G

I

K

L

M

R

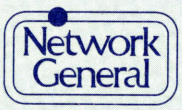
S

T

U

V

W



We solve network problems.™

Network General Corporation
4200 Bohannon Drive
Menlo Park, California 94025
(415) 688-2700

Network General Europe
Belgicastraat 4
1930 Zaventem, Belgium
32-2-725-6030